



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 3 April 2014

**7464/2/14
REV 2**

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

LIMITE

**DATAPROTECT 43
JAI 149
MI 256
DRS 36
DAPIX 41
FREMP 40
COMIX 146
CODEC 720**

NOTE

from: Presidency
to: Working Group on Information Exchange and Data Protection (DAPIX)
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)
- One-stop-shop mechanism

Delegations will find below comments regarding the one-stop-shop mechanism.

TABLE OF CONTENT

| | |
|------------------------|------------|
| BELGIUM | 3 |
| DENMARK | 10 |
| IRELAND | 18 |
| SPAIN | 22 |
| CROATIA | 36 |
| LUXEMBOURG | 39 |
| HUNGARY | 47 |
| POLAND | 50 |
| PORTUGAL | 57 |
| ROMANIA | 97 |
| SLOVAK REPUBLIC | 98 |
| FINLAND | 102 |
| SWEDEN | 108 |

BELGIUM

| |
|--|
| DAPIX MEETING – 18-20 February – ONE STOP SHOP – BELGIAN COMMENTS ON THE DOCUMENT 5882/2/14 |
|--|

GENERAL COMMENT:

BE wants to thank the presidency for the new text and the efforts to find a solution in that particularly important issue.

BE has received the German proposal and will send her comments on it directly to the German delegation.

As already said many times, BE is in favour of a one stop shop mechanism.

The key principle is to get one decision. The way of having this unique decision is another question. Within the text of the presidency, there is already a principle of close cooperation between the lead DPA and the DPA's concerned. A solution may perhaps be to go a little bit further in that cooperation and thus come closer to the codecision mechanism proposed by the French delegation. This would have as advantage of bringing citizens closer to the decision making process.

Lack of time for analysis requires us to put a **SCRUTINY RESERVATION**.

Nevertheless, in order to be constructive, we have some preliminary observations:

Concerning ART. 51a:

§3: *“Paragraph 1 shall not apply where the subject matter concerns only processing carried out in a single Member State and involving only data subjects in that Member State.”*

BE doesn't really understand the added value of this paragraph. This is the basis principle, no need to put it here.

§4: *“This article shall not apply where the processing is carried out by public authorities and bodies, including their processors, of a Member State. The only supervisory authority competent to exercise the powers conferred on it in accordance with this Regulation regarding a Member State's public authorities and bodies shall be the supervisory authority of that Member State”.*

BE welcomes this provision and wants also to cover processors that process the data on demand of public authorities. Proposition to add “including their processors”

Concerning ART. 54a:

BE is in favour of the reintroduction of the §4 which was about the inaction of the lead DPA. The previous version of the §4 was the following: *“Where the supervisory authority of the main establishment of the controller or processor does not act on a draft measure referred to in paragraph 2 of Article 54a, within a period of four weeks after having received the draft measure, the supervisory authority which has referred the matter in accordance with paragraph 1a of Article 51, may submit the matter to European Data Protection Board under the consistency mechanism referred to in Article 57.”*

Concerning ART. 54b:

§2: *“In a case referred to in paragraph 1 or 2 of Article 51a the supervisory authority to which the complaint has been lodged, Within the cases with a transborder dimension, where the subject matter of the complaint concerns only processing activities of an establishment of the controller or processor in one single Member State and the matter does not affect data subjects in another Member State, the supervisory authority to which the complaint has been lodged may, where appropriate, seek an amicable settlement of the complaint. Where such amicable settlement cannot be reached or where such an amicable settlement would not be appropriate, the supervisory authority to which the complaint has been lodged shall refer the matter and the result of its related investigations to the lead supervisory authority, which shall act pursuant to points (b) and (c) of Article 54a(2)”*.

BE is in favour of the introduction of §2. However, BE thinks that this paragraph is not clear enough and needs some improvements. For example, the beginning of the paragraph can be change by adding “within the case with a transborder dimension”.

Two informations need to be add:

1. information of the lead DPA when a local DPA considers that it is a national case: that will allow the lead DPA to check if there are no other similar cases.
2. information of the lead DPA about the terms of the amicable settlement: that will allow the lead DPA to advise or help another local DPA which might encounter the same problem a few years later.

§4: *“Where, in the case referred to in paragraph 2, the concerned supervisory authority to which the complaint has been lodged considers the complaint as unfounded, it shall notify this to the lead supervisory authority. Where the lead supervisory authority objects to such finding, it may refer the case to the consistency mechanism within two weeks after having received the notification. Where a supervisory (lead?) authority concerned has not objected within this period, it is deemed to be in agreement with the draft measure”*.

In order to well understand this §, BE asks herself if the reference to supervisory authority in the end of the §4 means the “lead authority”.

Finally, BE considers that the principle of the one-stop-shop, as stated by the presidency, lacks some rules :

- What is the effect of a decision taken by a lead DPA on the other establishments of the same controller?
- What are the guarantees that can ensure that a local DPA or a judge will be able to enforce a decision of a foreign DPA?
- What is the statute of the EDPB?

BE wants to thank the German delegation for his proposal on the one-stop-shop mechanism. It has the merit of bringing new ideas which is particularly welcomed in so far as we are a bit stuck in the negotiations on this issue.

As you already know, BE is in favour of the one-stop-shop mechanism. This is a very important issue that deserves an in-depth reflection in order to keep in one hand the unique decision for the companies and in the other, the proximity for the citizens.

You'll find below the preliminary comments of the Belgian delegation. We need more time to be sure to measure the exact impact of the proposal in practice.

1. Concerning the EU wide compliance procedure

- Concerning the scope of the compliance decision: This procedure is envisaged for the review of specific or planned processing activities by the companies. Does that mean that a company may have either a compliance decision for a part of its activities or the whole processing activities?
- Do the lead DPA have the possibility to refuse the application of a company? If yes, in which cases?
- The principle of the "lead authority" stay the same as the one proposed by the presidency. We can support this. But we cannot support the criterion for the main establishment. We prefer to keep the idea of the place where the decision are taken. We also support the introduction of the possibility to have this procedure for the representative in the EU. More generally, we think that the one-stop-shop should be applicable also to the representatives.
- The consultation of the national DPA's through the EDPB is, in our view, too heavy. We think that it would be faster and more efficient to target the national DPA's concerned.

- Concerning the delay for the lead DPA: We wonder whether it is realistic to envisage that a national DPA (which is the lead) will be able to analyse the processing activity or activities concerned and provide a draft compliance decision within 2 months. On the other hand, we understand the need for a quick decision process.

- If the draft decision issued by the lead DPA received no objections by the national DPA's within 6 weeks, all the DPA's are bound by this decision. We cannot exactly see what is the difference between this and a decision taken by the lead DPA in cooperation with the local DPA's, as it is proposed by the presidency. In the end, it's always a decision of the lead DPA which is binding for the national DPA's. The problem of independence remains, in our view.

- We can support the idea of giving legal personality to the EDPB.

- The process after the objection of a national DPA to the draft decision of the lead DPA is a bit complicated. If we understand correctly, if only one national DPA objects to the draft decision of the lead authority, the cooperation procedure may be launch. What if it's not the case? Moreover, the cooperation procedure creates a voting procedure but the DPA's have to vote on what? On the draft of the lead DPA or on the a new draft of the EDPB? It's also difficult, after a long procedure, not to reach a solution for the company concerned. Just inform the company of the result of the cooperation procedure is a bit too light. Recommendations issued by the cooperation procedure need to be given to the company as well in order to give to the company the opportunity to adjust its rules or methodology. This will avoid that a company has to do the process all over again with a risk to obtain the same result as before.

- Concerning the possibilities of legal redress for the citizens: national DPA's will be put in a very difficult situation. It's not that usual to have a data subject which bring an action to compel the DPA to intervene. Moreover in a case where the DPA is bound by a decision taken at an EU level.

- We need, for the whole process, a mechanism of review of the compliance decision. We cannot give a compliance decision forever. Even if there are no complain by a data subject or no non-compliance procedure, it does not mean that all the processing activities remain compliant. It needs to be review regularly.

1. Concerning the non-compliance procedure

- the criterion to be lead authority in the non-compliance procedure are different than the one for the compliance procedure. This is a bit difficult in practice.
- We cannot see the element of the one-stop-shop in this procedure.
- As explained at page 6 of the document, if a DPA initiate a non-compliance procedure, the company may apply for a EU-wide compliance procedure. Initiating a compliance procedure suspends the non-compliance procedure. This is not feasible. This is going to be used for bypassing the non-compliance decision. A non-compliance process should not be suspended by the initiating of a compliance procedure.

DENMARK

The one-stop-shop principle in the proposal for a General Data Protection Regulation (GDPR)

Denmark has several times voiced concerns regarding a constitutional problem due to the proposed one-stop-shop principle in the GDPR. The problem has been raised in the DAPIX working party, in Coreper and at Council meetings. The Danish constitutional concerns have been based on the understanding that a decision by a “lead authority” in one Member State would be directly binding for the concerned establishments in all Member States.¹

However, at the DAPIX working party meeting on 18-20 February 2014 the Commission and others clearly stated that a decision by the “lead authority” should be directed towards the “main establishment” and should only be binding for this establishment. It would then be for the “main establishment” – e.g. through internal business/cooperation rules – to implement the decision in subsidiaries in other Member States.

If it is the case that a decision by a “lead authority” in another Member State is not to be binding for e.g. an establishment in Denmark, Denmark will not have a constitutional problem with the one-stop-shop principle. In this case the principle would not entail the transfer of powers from Danish authorities to authorities in other Member States. It is however crucial that there can be no doubt that this is the case. The clarity on this point is not sufficient in the current draft.

On this basis, Denmark puts forward the following amendments and proposals to the relevant recitals and articles²:

(The proposals are based on the Presidency text in **5885/3/14**. New text is marked in **bold**. Text to be deleted is ~~crossed~~.)

¹ For a description of the Danish Constitutional problem, please see written comments dated 25 November 2013, reproduced at the end of this contribution.

² The remarks only refer to the abovementioned subject and are without prejudice to comments on other articles (and recitals) in chapters 6 and 7.

Recital 96a

Where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State or where the processing of personal data takes place in the context of the activities of one establishment of a controller or processor in the Union and the processing substantially affects or is likely to affect substantially data subjects in more than one Member State, one single supervisory authority should act as lead authority ~~and decide on measures intended to produce legally binding effects towards the controller or processor.~~ Within its tasks to issue guidelines on any question covering the application of this Regulation, the European Data Protection Board may issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State.

A supervisory authority should not act as lead supervisory authority in local cases where the subject matter concerns only processing carried out in a single Member State and involving only data subjects in that Member State. **The provisions on lead supervisory authorities should not apply for processing carried out by public authorities or bodies.** ~~This should also not apply where the processing is carried out by public authorities and bodies of a Member State. In such cases the only supervisory authority competent to exercise the powers conferred to it should be the supervisory authority of that Member State.~~

DK Remark

The last sentence of recital 96a seems to imply that in cases where the processing is carried out by others than public authorities, there will be cases where other supervisory authorities than the one of the Member State in question would be competent to exercise the powers conferred to it. This should however not be the case.

Recital 96b

The lead authority should be competent to decide on measures applying the powers conferred on it in accordance with the provisions of this Regulation. In its capacity as lead authority, the supervisory authority should cooperate with the supervisory authorities concerned.

The decision by the lead authority should be directed towards the main establishment as defined in this Regulation and should only be binding for this establishment.

Article 51

Competence

1. Each supervisory authority shall be competent on the territory of its own Member State to perform the duties and to exercise the powers conferred on it in accordance with this Regulation, ~~without prejudice to Article 51a~~
2. (...)
3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

DK Remark

If the decision by the “lead authority” is to be directed towards the “main establishment” and *only* be binding on this establishment, the wording in paragraph 1 “without prejudice to Article 51a” is misleading. The wording would suggest that in some cases a supervisory authority of another Member State would be competent to perform duties and exercise powers on the territory of the Member State mentioned in the article.

Article 51a

Competence for ~~acting as~~ the lead supervisory authority

1. **Without prejudice to Article 51**, where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State, the supervisory authority for the main establishment shall act as lead supervisory authority and shall be competent to decide on measures applying the powers conferred on it **in accordance with [Article 53...]**¹.

The lead supervisory authority should comply with the cooperation procedure foreseen in Articles 54a and 54b.

2. **Without prejudice to Article 51**, where the processing of personal data takes place in the context of the activities of one establishment of a controller or processor in the Union and the processing substantially affects or is likely to affect substantially data subjects in more than one Member State, the supervisory authority of that establishment shall act as lead authority and shall be competent to decide on measures applying the powers conferred on it **in accordance with [Article 53...]**².

The lead supervisory authority should comply with the cooperation procedure foreseen in Articles 54a and 54b.

3. Paragraph 1 shall not apply where the subject matter concerns only processing carried out in a single Member State and involving only data subjects in that Member State.
4. This article shall not apply where the processing is carried out by public authorities and bodies of a Member State. ~~The only supervisory authority competent to exercise the powers conferred on it in accordance with this Regulation regarding a Member State's public authorities and bodies shall be the supervisory authority of that Member State.~~

¹ The scope of the one-stop-shop should be further scrutinized in DAPIX.

² Cf. footnote 3.

Article 51b

Decisions by the lead supervisory authority

Decisions by the lead supervisory authority shall be directed towards the main establishment, as defined in Article 4 (13), and shall only be binding for this establishment.

Regarding the Danish Constitution and the one-stop-shop mechanism as proposed in the General Data Protection Regulation (25 November 2013)

During the negotiations of Chapter VI and VII in the General Data Protection Regulation, Denmark has several times voiced concerns regarding the one-stop-shop mechanism which provides that a supervisory authority in one Member State can take decisions that are directly binding in all Member States.

Our primary concern is that the Danish Constitution does not allow for Denmark to submit powers or competences that belong to Danish authorities to authorities in other countries. Denmark can therefore not accept that authorities in other Member States take decisions that are directly binding for citizens or businesses in Denmark as if the decisions were taken by Danish authorities. This gives rise to serious constitutional concerns in Denmark.

Denmark can therefore not support a proposal that provides for powers or competences, e.g. the power of taking binding decisions for citizens and businesses in Denmark, to be transferred to supervisory authorities in other Member States.

The problem is not one of enforcement. It is the mere fact that there is an authority in another country taking decisions that are directly binding for citizens and businesses in Denmark.

The text as it is now (*doc. 16626/13*) leads to the conclusion that decisions from the lead authority will be binding in all Member States. This is confirmed by the text and indeed the latest discussions in the DAPIX Working Party. It was stated that it is the cornerstone of the one-stop-shop mechanism that the decisions by the lead authority be binding for the main establishment, but also have to be followed by subsidiary companies in other Member States. It is for the local/national supervisory authority to ensure that the decision by the lead authority is being followed, because it is binding, and – if the decision is not followed – enforce it on its own territory.

As Denmark will have a constitutional problem if the lead authority in another Member States takes decisions that are directly binding for citizens and businesses in Denmark, it is crucial for us that this will not be the case if the one-stop-shop mechanism is agreed upon. Therefore it must be stated clearly in the text that decisions by the lead authority have to be approved or recognised by the local/national supervisory authority as a precondition for being binding in that Member State.

As the text is now, Articles 51, (1a) and (1b) (*regarding the exclusive competence of the lead authority*) in conjunction with other Articles such as Article 57 (2) (*“measure aimed at producing effects in more than one Member State”*) and Article 63 (1a) (*“to the controller or processor concerned”*) do not present the sufficient clarity to conclude that the one-stop-shop mechanism will not have serious constitutional concerns in Denmark. The Articles mentioned in their present wording on the contrary lead to the conclusion that decisions taken by a lead authority will indeed be directly binding for citizens and businesses in other Member States.

Therefore Denmark puts forward the following wording for an article to be included in Chapter VI ensuring that decisions taken by the lead authority are not binding in other states without the recognition of the local/national supervisory authority:

Article 51

- 1bb.** Adoption of measures by the supervisory authority competent for the supervision of the main establishment of the controller or processor referred to in [51 (1a) and (1b)] is binding in other Member States as soon as the supervisory authorities in the Member States concerned have recognised the decision without any further formality being required.

To conclude, if there is to be a one-stop-shop mechanism it should be clearly stated that it is a precondition that the decisions by the lead authority are recognised by the local/national supervisory authority. This is crucial for Denmark, because of the above mentioned constitutional concerns.

If it is not the case that decisions taken by the lead authority are to be directly binding for citizens and businesses in other Member States, this should alternatively be made clear in the text in order to exclude any doubt on this issue.

IRELAND

1. As already outlined at the DAPIX meeting 12/13 March, Ireland broadly supports the Presidency's proposals for a meaningful 'one-stop-shop' (document 5882/3/14 Rev 3). Ireland supports a model based on effective consultation and cooperation between the lead and the concerned supervisory authorities – where appropriate through use of the consistency mechanism – and remains opposed to the granting of legal personality and binding powers to the European Data Protection Board.
2. Ireland welcomes, in particular, local resolution of issues where only data subjects in a single Member State are involved (article 51a.3) and amicable resolution where that is appropriate (article 54b.2). This will reduce recourse to the lead supervisory authority.
3. Ireland can also support the view that legally binding measures taken by the lead supervisory authority should apply to the controller's or processor's main establishment (e.g. imposition of fines). Where such measures require implementation in other Member States (e.g. an order to bring processing operations in several establishments into compliance with the Regulation), the mutual assistance mechanism in article 55 should be used.

Specific comments

4. Detailed suggestions regarding text as follows:
 - a. In paragraphs 1 and 2 of article 51a, consider replacing “shall be competent to decide on measures applying the powers conferred on it ...” with “shall be competent to exercise the powers conferred on it...”
 - b. Ireland is not convinced of the usefulness and viability of the 'partial' public register referred to in paragraph 1 of article 51b (such a register would not be comprehensive since it would only include disputed cases).

- c. Ireland considers that subparagraph (ab) of paragraph 1 of article 52 is a ‘power’ rather than a duty (i.e. a general power to intervene on any issue related to the protection of personal data). On the other hand, the supervisory authority must have a duty to respond to consultations under article 34.7. Subparagraph (ab) should, therefore, be replaced with the following: “respond to consultation requests on legislative and administrative measures relating to the processing of personal data pursuant to article 34.7”.
- d. Subparagraph (k) of paragraph 1 of article 52 (“issue opinions as well as fulfil other duties related to the protection of personal data”) is much too vague to be a duty; on the contrary, consideration should be given to converting it into a power under article 53 (see g. below).
- e. In article 52.4, the words “by measures which can be completed electronically” are unclear. We suggest replacing the word “measures” with “a form” (the intention here, presumably, is to allow electronic submission of complaints).
- f. Article 52.5 requires that supervisory authority services shall be free of charge for data subjects and data protection officers. Does this mean that supervisory authority services are not free of charge to controllers? (e.g. where a controller consults the supervisory authority under article 34.2, or the authorisation of contractual clauses under article 42.2(d)).
- g. Under article 53, the supervisory authority should have a general power to issue opinions on any issue related to the protection of personal data.
- h. In article 53a, paragraph 2, insert “it takes” (i.e. “In particular, each measure it takes shall:”); in subparagraph (b) replace “him or her” with “that person” (i.e. must include legal persons as well as natural persons).
- i. In paragraph 3(c), replace “time of issuance” with “data of issue”; in paragraph 3(f), delete all words following “effective remedy” (i.e. avoid imposing an excessive burden on supervisory authorities).

- j. In article 54b.5, insert “authority” after “supervisory” in line 2.
- k. Consideration should be given to having a standard time limit in these articles instead of 4 weeks (article 54a.3; 54b.3), 2 weeks (article 54b.4; article 61.4), one month (article 55.2; 55.8; article 58.7); perhaps periods of 4 weeks and 2 weeks would be sufficient.
- l. In paragraph 56.3, replace “in so far as the host supervisory authority’s law permits” with “in so far as the law of the Member State of the host authority permits”; also replace “seconding supervisory authority’s law with “the law of the Member State of the seconding authority”.
- m. In article 56.3c, it is not clear what exactly “damages it has sustained” is referring to; this needs to be clarified.
- n. Ireland has considerable doubts about the legality of the proposal in article 62.1(a); while the Commission enjoys infringement powers, it cannot be appropriate to intervene in specific cases in this manner.
- o. In article 73.1 replace “with a supervisory authority” with “with a single supervisory authority, in particular in the Member State of his or her habitual residence or place of work”.

German paper

- 5. As regards the proposals submitted by Germany, Ireland is not opposed in principle to a voluntary procedure on the general lines of the proposed article 34a, on condition that this is without prejudice to the duties and powers of the competent supervisory authorities.
- 6. Any ‘Union-wide legally binding decision’ under the compliance procedure, would of necessity require a willingness on the part of supervisory authorities to commit to giving a ‘green light’ to specific processing operations. The legal and practical difficulties associated with this type of commitment have already been discussed in the context of article 34.3.

7. Other elements of the proposed model appear to be much more complex and resource-intensive, including for the European Data Protection Board. As already earlier, Ireland does not support the granting of binding powers to the Board.

8. Finally, the proposal that the decision of the lead supervisory authority is binding only for the supervisory authorities which have agreed with it would lead to legal uncertainty and fragmentation of the EU, contrary to the objectives of the Regulation.

SPAIN

The Spanish delegation would like to thank the Presidency for its last proposal and to welcome the Presidency's initiative of opening the debate in this subject to other approaches.

General comments

Although we appreciate the obvious efforts made by the Presidency to solve some of the problems our delegation (among others) have been raising during the DAPIX discussions on one-stop shop, we believe that this paper does not fully address most of our concerns. In fact, we do not perceive a significant progress compared to previous proposals on the subject. Therefore, the main demand of our delegation, the lack of proximity, still upholds.

Lack of proximity

We understand that the Presidency's proposal purpose of introducing proximity in the one-stop shop mechanism is basically contained in arts. 51a.3, 54b and 74.2 and 3.

Art. 51a.3 refers to what has been improperly called "local cases". According to this article, when the subject matter of the procedure concerns only processing activities carried out in a single Member State and involving only data subjects in that Member State, the "lead DPA" principle shall not apply, and therefore, the "local" DPA shall be competent to deal with these cases.

Art. 54b establishes three different ways to supposedly introduce proximity. Firstly, it allows the local DPAs to reach an amicable settlement of the complaint with the controller or processor, even if the competence resides on the lead authority according to art. 51a.1 and 2 (ex art. 54b.2).

Secondly, it should be possible for the data subject to appeal against the inactivity of his or her local DPA, in case the decision of the lead DPA is contrary to the data subject's interest and the local DPA does not object (art. 54.5). This inactivity would supposedly produce an administrative act (by administrative silence) that could be appealed before the courts of the Member State where the local DPA is established (art. 74.3). Finally, the Presidency's proposal establishes that when the local DPA (with the agreement of the lead DPA) understands that the complaint is unfounded, it shall reject the complaint and notify the rejection to the complainant (art. 54b.4 and 5). Therefore, this "rejection" could be appealed by the data subject before the courts of the Member State where the local DPA is established (art. 74.3).

As regards **art. 51a.3**, the Spanish delegation believes that the definition of “local” or “minor” cases is too restrictive and does not cover all situations where national DPAs that are not “main establishment DPA” should have competence to decide cases that have not a transborder impact. With this definition, many cases with only local impact will have to be sent to the lead DPA. In particular, all cases where there is inadequate implementation at the local level of processing operations that are designed for and applied in all the Member State where the company operates.

We would be in favor of a definition based on the original cause of the problem. Where the potential infringement is the result of decisions, implementing measures or actions at the national level the competence should be of the national DPA.

Furthermore, we understand that the scope of this paragraph is heavily undermined by art. 54b.2. At first, it appears that in the cases where art. 51a.3 applies the lead DPA does not intervene. Nevertheless, art. 54b.2 establishes that *even* where art. 51a.3 is to be applied, the lead authority still has an important role to play in the procedure. In fact, the competences and powers of the local DPA are substantially reduced: they may reach an amicable settlement to the complaint, reject the unfounded complaints (with the agreement of the lead DPA) and object the draft proposal of the lead DPA. In sum, even in local or minor cases, the local DPA is not allowed to decide in most cases, and when it is allowed, they require the endorsement of the lead DPA. Thus, the “proximity effect” sought by this article is not fulfilled.

Finally, we must take into account that in the rest of the cases, in the ones referred to in art. 51a.1 and 2, the only competent authority to make the final decision is the lead DPA. This is clearly stated by art. 54a.1, as it words that “In the cases referred to in paragraphs 1 and 2 of Article 51a, (...) the lead supervisory authority(...) shall cooperate with the supervisory authorities concerned by the processing in question in accordance with this article and with Article 54b in an endeavour to reach consensus”. The lead DPA is obliged (shall) cooperate in an endeavour to reach consensus, but the opinion or other DPAs has no substantive effect on the final decision, apart from opening the way for the implementation of the consistency mechanism, where decisions made by the EDPB are not binding.

As for the proximity supposedly ensured by **art. 54b**, we would like to highlight the following aspects:

- A. The mere possibility to reach an amicable settlement of the complaint granted to the local DPA does not fulfill the mandate of the JHA Council of October 2013 to the DAPIX Group to introduce proximity in the Regulation.

- B. The possibility of appealing against an act based on administrative silence or failure to act when the local DPA does not object a lead DPA decision that is contrary to the data subject's rights is highly problematic:
 - 1. We do not understand how could there be administrative silence of the local DPA when taking the final decision of the procedure is competence of the lead DPA. The decision of the local DPA not to object to the draft proposal is a process act, not a final act of the procedure, because as art. 54b.4 states, the non-objection of a local DPA must be understood as an agreement with the *draft* measure. Therefore, there is still no final act to appeal against; this "silence" is still a process act. And if there is no final act, there is no possible appeal before the courts of the Member State where the local DPA is established. That is to say, no proximity effect.
 - 2. The possibility to object is not an obligation to respond the data subject's complaint (which reside, as the competent DPA, on the lead authority), and thus, the administrative silence cannot be applied to the "inactivity" of the local DPA.
 - 3. Anyway, art. 74.2 does not allow the data subject to appeal against the "administrative silence" of its DPA before the courts of the Member State where this DPA is established, because this DPA, the local DPA, is not competent.
 - 4. Even if the administrative silence could be applied in these cases, a main element of proximity would not be achieved because the final decision is still competence of the lead DPA; and not only will this DPA decide basing on the Regulation, but it will also make use of different laws, maybe national laws (for example: labor laws), to make its decision. Can we presume that i) the local DPA will have legal arguments to object against a decision based on foreign laws, and ii) the data subject will understand a decision based on foreign law?

- C. The power to reject unfounded complaints is also problematic. We understand that “reject” stands for what in Spanish administrative law is “non-acceptance” (inadmisión), that is to say, when the administrative body does not consider the heart of the matter of the citizen’s complaint. But, what happens when the DPA does not “reject” (in the abovementioned sense) but “dismisses” the complaint because the controller or processor has not infringed the Regulation? What DPA is competent for “rejecting” in the sense of “dismissal”?

Anyway, we cannot support the distribution of decision making competences foreseen in this article in relation to “local cases”. On the one hand, we cannot find legal grounds to attribute competences on the basis of the content (positive or negative) of the decisions.

Additionally, there are many cases where the final decision is not clearly positive or negative but has mixed effects. Finally, the fact that the decision of the local DPA has to be “verified” or “approved” by the lead DPA may very well question the possibility to challenge it before the national courts of the data subject. Particularly in cases where the local DPA has changed the content of the decision as a result of the opinion of the lead DPA or where the local DPA considers that the complaint is founded and the lead DPA disagrees.

Finally, the actual proposal does not take into account the possibility that the lead DPA agrees with the complainant, and the controller/processor decides to appeal against the court of the Member State where the lead DPA is established. In this case, the data subject will have great difficulty to enter in appearance before the courts of another member State.

Other comments

We would like to clear out a comment done by this delegation during the last DAPIX meeting that we believe was misunderstood by the Presidency, probably due to the interpretation. Regarding art. 52.1ab, we stated that we would be in favour of qualifying the obligation to provide information to “other political institutions” with a reference to national law. The expression “political institution” is too vague and may include many entities which, according to national legal systems have no specific right to be regularly or formally informed by DPAs. For instance, in politically decentralized Member States national DPAs may not be obliged to provide information to regional parliaments or to local councils, which are obviously “political institutions”.

On the contrary, we are not against the obligation of national DPAs to provide information to their national parliaments, as the presidency suggested after our intervention in the discussions.

Conclusion

Although the proposal is well-intentioned, we do not share the views that it complies with the mandate of increasing the proximity expressed by the JHA Council to the DAPIX Working Group. The main concerns that this delegation have raised in the meetings regarding the lack of proximity of the one-stop shop mechanism still remain. Therefore, please note that Spain has a negative scrutiny reservation on the whole 5882/3/14 REV document.

German proposal for the one-stop-shop mechanism

The Spanish delegation wishes to thank the German delegation for its alternative proposal on the one-stop shop mechanism. We would also like to welcome the Presidency's initiative of opening the debate in this subject. From our perspective, with this new approach it might be possible to deal with certain issues that have been raised by different delegations throughout the DAPIX discussions on one-stop shop.

General comments

In principle, Spain supports some of the core ideas of the German proposal:

- The identification of the main establishment based on criteria which are more objective and predictable than the internal decision making process to which former proposals refer.
- The recognition that competence of DPAs not only may be based on the existence of an establishment of the controller or processor, but also on the presence of residents affected by the processing operation (i.e.: criterion of offer of products or services, plus monitoring of behavior).
- The preservation of the competence of "national" DPAs to decide on procedures related to the possible "non-compliance" of controllers or processor, be it as result of a complaint lodged by data subjects or as a consequence of an "ex officio" investigation.
- The idea of harmonization as a result of collective decisions ("compliance" and "non-compliance" procedures) that respect the competences of national (or "local") DPAs.

Nevertheless, we still have certain misgivings about some of the elements of the proposal. In this regard we would welcome further clarifications on the following aspects:

- What is the scope of "compliance" decisions?
- What is the relationship (or the difference) between "compliance" decisions and certifications or adherence to codes of conduct? Do they have the same consequences? Could it be that the alternative possibility of having "compliance" decisions issued by DPAs makes certifications issued in accordance with Art. 38 of the draft Regulation less attractive for companies?
- What might be the impact in terms of additional workload for DPAs?
- EU wide "compliance" and "non-compliance" procedures lead to decisions that are only generally binding if all members of the EDPB accept the draft decision submitted by the lead(requesting) DPA (or partially binding for those DPAs that have not objected to the draft). That being the case, what is the purpose of this procedures if a co-operation procedure may be initiated by any of the affected parties where real "collective" decisions may be made that do not always need require unanimity of EDPB's members may be adopted?

- The possibility that the controllers may suspend a “non-compliance” procedure by lodging a request for a “compliance” procedure raises many doubts with regard to its purpose, its relation with national and EU wide procedures and its consistency with national administrative legal frameworks.
- What would be the legal procedure to give legal personality to the EPDB? And for eventually attributing the ECJ competences for challenging the decisions of the EPDB?
- What is the relationship between “non-compliance” decisions (at both the national and the EU level) with sanctions? For instance, if a EU wide decision of “non-compliance” has been agreed on by all or a number of DPAs, may all of them sanction the controller at the national level on the basis of the EU wide decision (provided that they also have opened procedures regarding that controller and that infraction), or is that possibility only available to the national requesting DPA?

Art. 34a

Article 34a

Decision on Compliance

- 1. Controllers, processors, joint controllers or group of undertakings which have their main establishment in the Union or have designated an representative pursuant to Art. 25 (applicants) may on request obtain a Union-wide compliance decision in trans-border cases from the competent supervisory authority, in order to ensure the compliance of data processing with this Regulation.**
- 2. In order to obtain a compliance decision the applicant shall make a request to the supervisory authority. In the request the applicant must describe and explain**
 - (a) the controller, processor, joint controllers or group of undertakings to which the decision shall apply,**
 - (b) the category of data processing practised or planned,**
 - (c) the concrete concept that the data processing is based on and that is to be examined in the compliance procedure,**
 - (d) the legal basis of the data processing pursuant to Article 6 and the measures to protect the data subject pursuant to this Regulation.**
 - (e) the data protection impact assessment as provided for in Article 33 indicating that the processing is likely to present a high degree of specific risks,**

(f) a reasonable interest

aa) in a compliance decision, for example in the case of the introduction of new data processing or a processing for which no established practice or, clear opinion of the supervisory authority exists and

bb) in a Union-wide decision, notably the importance of the data processing for a substantial number of data subjects concerned in more than one Member State or the existence of establishments in more than one Member State.

The Spanish delegation has some doubts with regard to the scope of the “compliance” procedure in art. 34a:

- What is to be declared as compliant? Processing operations, products or services, the company as such? The article refers to “trans-border cases” and “data processing” but does not specify what should be understood by these expressions.
- The article refers to companies with their “main establishment” in the EU and to “trans-border cases”, but also to “compliance decision” as opposite to “EU wide compliance decision (par. 2.f). Does this mean that there are two types of compliance decisions, one limited to the territory of a Member State and another one of EU-wide character?
- Is it possible to apply for a compliance decision with regard to any data processing operation or is that possibility limited to data processing operations that have to be subject to a DPIA and which present a high degree of specific risk (par. 2.e)?
- It seems that a company may request a compliance decision at any time during a processing operation. Is it necessary to justify why a request is lodged after the processing operation has been in place for some time (apart from cases where a non-compliance procedure has been launched by a DPS)?

Art. 51.1.b

b) processing **which is related to the offering of goods and services to data subjects on its own Member State by controllers not established in its own Member State;**

Is this concept meant to replicate the one used in art. 3.2 of the draft Regulation? If that is the case, in order to avoid discrepancies it would be advisable to include a reference to the monitoring of the behavior of data subjects as well.

Article 52a

Cooperation and mutual assistance between supervisory authorities

1. The supervisory authorities of the Member States shall provide each other with all useful information, analysis and mutual assistance on questions of fact or law in order to implement this Regulation in a consistent manner.
2. The lead authority shall, without undue delay, provide the other competent supervisory authorities with all relevant information and analyses obtained while performing its duties. Any competent supervisory authority may also request relevant information and analyses from the lead authority.
3. The European Data Protection Board shall be used to facilitate the cooperation and the exchange of information. Therefore the European Data Protection Board could establish a situation centre with liaison officers from the supervisory authorities of the Member States.
4. For the purposes of applying the provisions of this article, the supervisory authorities and the European Data Protection Board shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.

This provision and the system as a whole seem to lead to the permanent involvement of DPAs in the decision-making process and to a massive exchange of information and documents among DPAs as well. This implies a heavy burden (time, translations, staff, etc...) and costs that might be difficult to bear by some, if not many, DPAs. It could be a weakness of the proposal. It is true that any model based on a strong cooperation among DPAs will have similar problems. In order to address them, it would be advisable to limit the scope of the system to the minimum possible, maybe to those “important transnational cases” mentioned by the JHA Council in October.

Art. 56.5.b

If the lead authority considers that the data processing of the applicant does not comply with the applicable data protection law, it shall reject the request for a compliance decision. This rejection is legally binding in the territory of the Member State of the lead authority. The lead authority shall decide after due consideration whether to initiate a non-compliance procedure pursuant to Article 57.

What is the reason for not making it mandatory to initiate a EU non-compliance decision? If the company applied for a EU-wide compliance decision it seems reasonable that the answer, either positive or negative, should have in any case EU-wide nature.

Art. 56.7

The participating supervisory authorities of the other Member States may comment on the draft compliance decision by the lead authority and/or object to it. Failure by a supervisory authority to respond within the six weeks' time limit set by the European Data Protection Board shall be deemed as a vote in favour of the draft (tacit agreement). The subsequent compliance decision by the lead authority shall be binding if all supervisory authorities of the Member States did not object. Objections shall set out the grounds for the decision to object. If one supervisory authority objects to the draft decision of the lead authority, any national supervisory authority, the European Commission or the European Data Protection Board may launch the cooperation procedure pursuant to Art. 58.

In case some DPAs object to the compliance decision, is it still possible for the lead DPA to adopt it with binding effect in a Member State where DPAs have not objected to the draft decision of the lead DPA? The last sentence leads to a different conclusion, but in theory nothing would prevent the decision from becoming binding in a number of Member States pending the result of the cooperation procedure that might make it binding in all Member States.

Art. 56a.2

Each data subject shall have the right to judicial remedy brought before the court of the Member State in which he /she is resident against its supervisory authority in case the supervisory authority refuses to take a measure due to a binding compliance decision. If the compliance decision was found in violation with the rules of this Regulation it shall not be binding for the supervisory authority of the Member State where the data subject has his/her residence. Each data subject shall have the right to judicial remedy against the decision of the European Data Protection Board brought before the General Court pursuant to Article 263 (4), Article 256 (1) TEU.

This article appears not to foresee one possible situation: a company has received a compliance decision with regard to a processing operation and still infringes the Regulation because of an implementation of the processing operation which is not in accordance with the terms under which the compliance decision was issued. In this case, the decision is correct, but the infringement exists. It seems reasonable to think that in those cases the national DPA may take a measure with regard to the infringement and that the national court may also issue a judgement with regard to the possible infringement and not to the “legality” of the compliance decision. If that is the case, it would be advisable to include it expressly among the redress scenarios, at both the judicial and the administrative level.

Art. 57.1

Each supervisory authority may initiate the Union-wide non-compliance procedure to obtain a legally binding decision by the supervisory authorities of all Member States if in its opinion a certain data processing activity does not comply with this Regulation. Each supervisory authority shall initiate the Union-wide non-compliance procedure to obtain a legally binding decision if the said processing activities are related to the offering of goods or services to data subjects in several Member States and may substantially affect the free movement of personal data within the Union or the right of individuals to protection with regard to the processing of personal data.;

The expression “legally binding” is a little misleading. In fact, the outcome of the “non-compliance” procedure would never be a “binding decision” of the EDPB. In the most optimistic scenario, it would be a unanimous acceptance of all DPAs of the draft submitted by the requesting DPA. That would make the decision binding in all Member States, but as a consequence of 28 binding decisions (each one with a limited scope) and not because of a “common” decision. Additionally, the scope of this provision does not seem to be consistent with that of Art. 51 of the proposal nor with the terms of art. 3.2 of the draft Regulation. The same applies for point 4.b of this article.

Art. 57.5

The requesting supervisory authority has to inform the controller or processor about the intention to initiate a Union-wide non-compliance procedure one month before the procedure starts. The information shall contain recommendations how to ensure the protection of personal data and to demonstrate compliance with this Regulation. The right of the controller to initiate a Union-wide compliance procedure with the lead authority pursuant to Article 56 remains unaffected. If a Union-wide compliance procedure is initiated the non-compliance procedure is suspended. In exceptional circumstances, where there is an urgent need to act in order to protect rights and freedoms of data subjects, the supervisory authority may immediately adopt provisional measures in accordance with Article 53 for the territory of its own member state, as long as the compliance procedure is going on.

This may be difficult to implement. If the requesting DPA has concluded, after an investigation carried out according to the national and European procedures and has found that the company has seriously infringed the Regulation, it would not always be appropriate, or at least in accordance with the administrative procedures in some Member States, to just issue “recommendations” to the company.

Additionally, we do not follow the logic of the EU-wide compliance request as a response to the EU “non-compliance” request initiated by the requesting DPA. It seems that what the company has to say against the arguments of the national DPA to consider that the company is not in compliance with the Regulation should be part of the national “non-compliance” procedure, and not the beginning of a different procedure. It is difficult to foresee how a company that has been found “non-compliant” with the Regulation at the national level may challenge that decision lodging something that looks like an appeal with automatic suspensive effect before the EDPB. Apart from that, it is not clear how the outcome of the EU compliance procedure will affect both the national “non-compliance” decision and the EU wide “non-compliance” procedure

Art. 57.8

The European Data Protection Board shall identify the result of the Union-wide non-compliance procedure after the deadline for submitting an agreement has passed. The Board shall inform the requesting supervisory authority, the supervisory authorities and the European Commission of the result of the Union-wide non-compliance procedure. The Board shall forward to the controller or processor in question all of the participating supervisory authorities' agreements and comments. The requesting supervisory authority shall inform the controller or processor of the result of the Union-wide non-compliance procedure.

It is not clear to us the purpose of informing the controller or processor of the DPAs’ agreements and comments.

Art. 57.9

In order to bring about a uniform, Union-wide opinion, the requesting supervisory authority, the European Commission or the European Data Protection Board may within one month initiate the co-operation procedure pursuant to Article 58.

It seems that, following the logic of the system, in case all DPAs accept the non-compliance decision it becomes the “uniform, Union-wide opinion” within the “non-compliance procedure” and the co-operation procedure is not necessary. If that is the case it might be advisable to word it explicitly.

Art. 58.1.b

if the Union-wide non-compliance procedure (Article 57) did not lead to a Union-wide binding decision,

Does “binding decision” mean that all DPAs have agreed with the respective draft decisions within the “compliance” and “non-compliance” procedures?

Art. 64.1

A European Data Protection Board is hereby set up. **It shall have legal personality.**

How will this become possible? Under which type of body?

CROATIA

Regarding the German proposal (document 6637/14)

Proposal of the German delegation has a solid basis, but according to the opinion of the HR, the whole proposed procedure needs to be simplified. We welcome the basic goal of establishment of the legal certainty for enterprises as well as proximity principle for the individuals on the other hand. We find appropriate classification of the authorities on the „supervisory authority“ (set up in every Member state) and „lead authority“ (as one of the supervisory authorities that would become competent according to the residence of the legal person or domicile of the individual). We welcome the role of EDPB in first stage. However, every of sub-methods connected with the procedure of co-operation needs to be simplified. Moreover, it remains unclear why in this kind of proposal the strengthening of EDPB role is not proposed. In described division of procedural steps, EDPB would likely take over the mandate which is in proposed draft of the Regulation vested to the body called „lead authority“.

Regarding the one-stop-shop mechanism we would like to thank the PRES for their efforts and the proposal presented. Nevertheless, it looks like that this proposal is subject to very different interpretations from the MS which could jeopardize the equal implementation of those provisions which is one of the principal goals of the Regulation as a legislative instrument .

In that context HR considers that the proposal of the DE delegation offers a quality basis for further work on one-stop-shop mechanism. Furthermore, generally in relation to the Regulation and especially in relation to the provisions that cover situations in more than one MS, HR is looking forward to further contributions in order to achieve a wide consensus among the MS.

Regarding the DE proposal we would like to point out the following:

- In relation to article 34a, HR considers that it's good to recognize the interest of the data controller, data processor and other subjects to receive a certification on compliance of their processing with the EU data protection provisions. However, HR considers it would be useful to transfer the art. 34a, par. 2, letter f, sub-points aa) and bb) to the recitals.

- With regard to the codes of conduct, in article 56, par. 1, letter b, we think instead of article 38(2) should be mentioned article 38(2b), since article 38(2) regulates the data processing in one member state, and 38(2b) regulates data processing in more than one MS. In the same article, in paragraph 6, HR considers that instead of 6a, 5a should be mentioned.
- According to article 56, paragraph 5, letter b, the lead authority could reject the request for a compliance decision and this rejection would be legally binding in the territory of the MS of the lead authority. From that provision it is understandable that the same data processing could be qualified as unsatisfactory in one MS (the MS of the lead authority) and satisfactory in the rest of the MS. Taking that into consideration, HR thinks such possibility wouldn't make possible the equal implementation of the Regulation and rises the question of the purpose of the Regulation (as an instrument that needs to provide equal rights to data subjects, equal rights and obligations to controllers, processors and others, and also equal praxis in the MS). Regarding the mentioned, HR proposes the adoption of a compliance decision by a minimum of 2/3 of the EDPB members, and at the same time providing to any unsatisfied MS the right to a judicial remedy before the Court of Justice of the EU.
- Regarding the article 56a, we consider it needs a new formulation since we find it unintelligible.
- HR doesn't agree with the first sentence of the article 57 paragraph 1 and thinks it needs to be deleted. According with that sentence there is a possibility to start the Union-wide Non-compliance Procedure even in cases where the data is processed only in one MS without any influence on others MS. HR considers that the data processing in such cases could be assessed only by the competent authority of that MS. In the paragraph 6 of the same article HR proposes to introduce the possibility of expanding the timeframe when there is a justified reason (case complexity, etc).

- HR considers there should be regulated the cooperation mechanism between the supervisory authority which started the non-compliance procedure and the supervisory authority that is in charge of the investigation (and which will later adopt the final decision). One possibility is to introduce in the Regulation the provision by which the EDPB would be entitle (and obliged) to adopt a general document regulating this cooperation.
- In article 58, paragraph 2, is needed to change the mention of article 56(8) since that provision doesn't exist. We think there should be a mention of article 56(6) or generally article 56.
- In relation to article 62 we are in favour of the provision taken from the document 17381/13, in regard with that provision we consider it does clearly define the COM competencies on implementing acts. HR also supports the provision of article 64 which gives legal personality to the EDPB.
- Regarding the right to lodge a complaint with a supervisory authority (article 73), HR thinks it would be a good solution to give to the data subject the right to lodge a complaint to the supervisory authority of the country he/she is resident or to the supervisory authority of the country where the infringement has occurred. HR points out there should be the possibility to lodge a complaint only to one of those supervisory authorities. In any case the supervisory authority of the country he/she is resident should actively assist the data subject in exercising his/her rights.
- Regarding the article 74 paragraph 4, HR considers the last two sentences need to be deleted. Also, it's important to emphasis that the judicial redress can be achieved only before the court which is competent to review the decisions of a certain supervisory authority (the courts of its MS).

LUXEMBOURG

Regarding document 5882/3/14.

General remarks

Luxembourg expresses its thanks to the Presidency for all the work put into drafting a balanced text on the one-stop-shop.

Luxembourg strongly support the principle of a one-stop-shop whereby one lead DPA, after consulting and closely associating concerned DPAs, takes a legally binding decision on the main establishment of the controller with EU-wide effect. According to Luxembourg, this allows for a win-win situation for both citizens and businesses: the former benefit from a same high level of protection across the EU (which they don't currently enjoy), and the latter gain legal certainty across the EU (which currently doesn't exist).

The proposal by the Presidency seems to guarantee these objectives to a very large extent, including proximity for data subjects. Luxembourg believes this text can form the basis for a mechanism acceptable for all and strongly urges the Presidency and all delegations to continue working on this basis.

Some comments aimed at improving the text are set out below.

Detailed comments

- Definition of 'main establishment': Luxembourg wishes to put a scrutiny reserve on the definition.

- Article 51a : Luxembourg largely supports the architecture of this article: paragraphs 1 and 2 cover the necessary cases for identifying the lead DPA. Going beyond these scenarios would dilute the efficiency of the one-stop-shop.

Luxembourg supports the scope of powers for the lead DPA.

According to Luxembourg's understanding, a decision taken by the lead DPA is imposed on the main establishment, and valid throughout the EU: it is implemented via the controller who ensures that all his dependent establishments conform to the decision by the lead DPA. This would be in continuation with the logic of directive 1995 where article 4(1)(a) reads: "... when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable." A similar provision could be included in this Regulation.

In paragraph 1, Luxembourg is not convinced that processors should have cumulative obligations with the controller. Further reflection is also necessary with regard to the impact on cloud computing.

In paragraph 2, Luxembourg supports the criterion of « substantially affect » and « likely to substantially affect ». To be more precise and to create coherence across the text, "data subjects residing in more than one Member State" should be added.

In paragraph 3, it should be clarified that its interpretation should be laid out narrowly in order not to potentially undermine the one-stop-shop.

- Article 51b: Luxembourg can support a public register for confirmed main establishments. Furthermore, the possibility should be given to controllers to designate themselves, in conformity with the objective criteria contained in the definition of 'main establishment', their lead DPA.
- Article 53a: Luxembourg can broadly support the content and objectives of this article.

- Article 54a: Luxembourg strongly urges to refine the second criterion determining a concerned DPA by making a plural as follows: “or where a significant number of data subjects residing in this Member State is likely to be substantially affected”. Just having one data subject likely to be substantially affected is too low a threshold. A quantitative criterion provides for more legal certainty and clarity in the procedure.

In paragraph 1a, Luxembourg wonders if this amounts to a right of initiative by the concerned DPA to launch the cooperation procedure. Does that mean that a concerned DPA can call upon a lead DPA to take action? Such a procedure seems confirmed by paragraph 2(ca) that requests a lead DPA to adopt a measure referred to it by a concerned DPA. This would undermine the concept of the one-stop-shop: the lead DPA would in fact not be “in the lead” anymore, but instead the concerned DPA.

In paragraph 3, Luxembourg would like to add that any objection by a concerned DPA should be duly justified and made on reasonable grounds in order to avoid unfounded objections. This will also allow for a better understanding of the issue tackled by a concerned DPA.

Luxembourg is also concerned that paragraph 4b may undermine or open the door to easy circumvention of the one-stop-shop.

- Article 54b: Concerning paragraph 2, Luxembourg supports the principle of amicable settlements of complaints. This allows for a more efficient procedure. Some additional provisions may be foreseen to inform the lead DPA on the issue of the amicable settlement (see comments from Belgium). Also Luxembourg wonders about the status or legal effect of the outcomes of amicable settlements.

According to Luxembourg paragraph 5 suggests a codecision model whereby both the lead DPA and the concerned DPA agree on a complaint that is unfounded. Luxembourg would rather see this as a decision taken by the lead DPA and recognized by the concerned DPA (which is closely associated in the decision-making process). This implies then (but may be clarified) that the data subject can exercise a right to judicial review in his own Member State (if this is where the complaint was lodged), thereby reinforcing proximity.

Luxembourg considers it useful to clarify that only one same complaint may be lodged once with one DPA in order to avoid multiple proceedings. However, the choice of where this complaint may be lodged should be left open for the data subject in respect of his specific situation and needs, and to avoid arbitrary lock-in, and just as directive 1995/46/CE currently allows it.

- Article 55: Paragraph 8 may lead to incoherence particularly in cases where a controller has several establishments in the Union. A provisional measure will only apply to one establishment (within the jurisdiction of the DPA) but not to other establishments, among them possibly the main establishment. Also, what happens if the provisional measure (which could be a temporary suspension of processing activities) has caused a prejudice to the controller? May he ask for compensation, is the DPA that took the provisional measure held liable?
- Article 56: Luxembourg suggests deleting the last sentence of paragraph 2 (see also written comments from 29.03.2013).
- Article 57 : In coherence with the remark on article 54a(3), Luxembourg suggests that an objection made by a concerned DPA should be duly justified and be made on reasonable grounds. It should be avoided that unfounded objections trigger the consistency mechanism.

- Article 62: Luxembourg continues to examine the possibility of giving legal personality to the EDPB and have it take binding decision: therefore a scrutiny reserve. A certain number of questions related to the budgetary, legal and organizational consequences of giving the EDPB legal personality need to be answered. Possibly, it may seem disproportionate to have the EDPB take decisions on small concrete cases. Furthermore, Luxembourg would prefer to encourage a sense of community among DPA rather than create opposition amongst them.
- Articles 73, 74 and 75 : Luxembourg is satisfied with the rights provided for the data subject which he is able to exercise mostly in the Member State of his residence. They constitute a significant step towards more proximity than is the case with the 1995 directive. It should not be forgotten that a DPA, irrespective of whether it is the one of the Member State of the data subject or not, has as its duty (and the duties are harmonised) to ensure the respect of the rules (which are harmonised) and to protect the data subject in conformity with those rules. They are the natural protectors of the data subject vis-à-vis the state and the businesses.

Regarding the German proposal (document 6637/14)

Luxembourg expresses its thanks to the German delegation for their proposal on the one-stop-shop.

Luxembourg strongly support the principle of a one-stop-shop whereby one lead DPA, after consulting and closely associating concerned DPAs, takes a legally binding decision on the main establishment of the controller with EU-wide effect. According to Luxembourg, this allows for a win-win situation for both citizens and businesses: the former benefit from a same high level of protection across the EU (which they don't currently enjoy), and the latter gain legal certainty across the EU (which currently doesn't exist).

However, Luxembourg is unsure whether the mechanism proposed by Germany is a true substitute or alternative for a one-stop-shop as currently contained in the Presidency text (5882/3/14). The objectives as stated above, to which Luxembourg remains attached, do not seem to be guaranteed. A large number of questions remain open and new problems arise. While Luxembourg could consider integrating some elements of the proposed mechanism into chapter IV, Luxembourg prefers to continue working on the Presidency version of the one-stop-shop, more likely to address and safeguard proximity and a same high level of protection for the citizen, and to bring more legal certainty and less administrative burden for controllers.

On the compliance procedure

- Luxembourg wonders whether the compliance procedure concerns an individual processing of data, or whether it covers more generally processing activities of a controller. Will one controller have to get numerous compliance decisions? It is also unclear how long a compliance decision is valid: what happens if certain conditions or modalities of the “authorized” processing change, will a new compliance procedure have to take place? How will the DPA know that changes in the processing have occurred?
- Luxembourg does not consider the criterion in paragraph 1(b) in article 51 as appropriate for defining competence. This de facto creates competence for 28 DPAs wherever there is a processing in the digital context (goods and services offered on the Internet are by nature not territory-bound), which is contradictory to a one-stop-shop and leading to confusion and complexity.
- Moreover, Luxembourg is reluctant to have all DPAs consulted via de EDPB on any draft compliance measure submitted by the lead DPA. This is not coherent with an efficient one-stop-shop, and risks overburdening both DPAs and the EDPB, at the expense of data subjects and controllers. In Luxembourg’s view, the EDPB should rather intervene as a last resort instance in case of conflict and not be the one-stop-shop.
- Luxembourg also sees a risk of parallel proceedings concerning a same data processing, since any controller, processor, representative or DPA can initiate the compliance procedure.
- The potential result will be different compliance decisions by different lead DPAs concerning similar processing cases, with more fragmentation and incoherence in the application of rules across the EU.

On the non-compliance procedure

- Luxembourg does not understand the articulation with the compliance procedure, and wonders whether both logics are compatible with each other (notably the role of the lead DPA), but also with the objective of creating a one-stop-shop.
- Luxembourg wonders how this procedure articulates with the imposition of sanctions and other corrective measures.

HUNGARY

Presidency proposal

1. Concerning the planned rules of the one-stop-shop mechanism (hereinafter referred to as OSS), Hungary still maintains its previously articulated general opinion, namely:
 - a. the OSS in its present form serves the interests of the controller, which is anyway in a dominant position compared to the data subjects, however, on the whole it does not have an obvious added value for the data controllers;
 - b. it leads to a much complicated and overly long procedure due to the obligation of the numerous consultation mechanisms between Member States which circumstance hinders the effective protection of the data subjects' rights. The legal redress procedure – launched by the data subject – can get stalled for several reasons which subdues the substantive level of protection and the violation of law can remain without prompt consequences;
 - c. numerous dispositions of the mechanism are unclear, thus the requirement for legal certainty cannot be fulfilled and the different interpretations of the ambiguous rules will lead to constant legal dispute.

2. In our opinion the question of jurisdiction is also ambiguous („substantially affect data subjects” – this criteria cannot be explicitly determined by the adequate authority) and the very same concern applies to the dispositions about the obligation of the consultation between Member States („measures intended to produce legal effects” – almost every measure taken by the authority has legal effects, e. g. the rejection of the complaint).
 - a. the administrative and financial burdens of the DPA's would be significantly increased due to the obligation of cooperation deriving from the mechanism, thus detracting financial sources and manpower from their substantive function as ensuring legal protection for fundamental rights;

- b. the activity of the European Data Protection Board would also on a large scale be determined by the OSS, because of the coordinational and opinion-giving tasks, which seriously makes it dubious whether it can allocate sources to the strategical questions in order to strengthen the unified application of the Regulation.
3. In regard to the above mentioned, Hungary is not able to support the Presidency proposal on the OSS. We still deem it necessary to find a different approach to tackle the requirement of proximity – that means that the local DPA should have exclusive corrective powers to deal with the complaints of the data subjects and the lead authority should be competent only in authorisation powers in transborder cases. This approach would ensure the principle of proximity to prevail even in the case of judicial review of the decisions.
4. Maintaining our general comments on the OSS, Hungary does not agree with the new text in Article 62. (1) (a). In our view it is a question of importance, which should be settled by the Regulation and not by the Commission.
5. We already mentioned it several times before that with regard to Article 76 (1a), Hungary is of the opinion that the right to lodge a complaint with the supervisory authority should be ensured for anybody, as in an „actio popularis” procedure.
6. At the same point we do not agree that a complaint can be lodged only in the case of data breach (Article 32 (1)). In our view it should be ensured in any kind of violation of the data protection law.
7. There are several disposals in the Presidency proposal which seem to be incorrect but, because of our general rejection, we do not deem it necessary to make further comments on it.

German proposal

In our opinion the German proposal pays due consideration to the report of the Council Legal Service and offers the right balance between interests of the data controller and processor enterprises and the protection of the rights and freedoms of the data subjects. In consideration of the abovementioned, Hungary supports continuing the work on the basis of the German proposal.

Specific remarks:

1. Hungary suggests to rephrase Article 34a (1) and Article 56 (1) in order to extend the scope of the provision to planned data processing as well, as it is duly stated in Article 52 (1) l).

The circle of applicants should also be extended in order to involve persons (natural persons as well), who cannot be considered data controller or processor at that stage.

2. It is not perfectly clear in Article 51 (1) b) and in Article 57 (1) why the text only refers to the processing related to the offering of goods and services to data subjects and not to the monitoring of data subjects as well.
3. We suggests to make it unambiguous in Article 51 (1) b) that under this point processing is carried out by controllers established in the EU, otherwise the scope of point b) and c) can not be separated unequivocally.
4. We would like to indicate that Article 52 (1) l) concerning the competence of the DPA does not correspond with Article 53 concerning the powers of the DPA (the latter contains no provision about non-compliance decisions).
5. It is not perfectly clear what sort of effect has the judicial redress regulated in Article 56a (2) and in Article 57a on the decisions of a DPA from another Member State, and where can find the data subject judicial redress if the violation occurred not in his/her state of residence but in another Member State.
6. Concerning Article 73, it is not perfectly self-evident at which DPA can the data subject lodge a complaint if the violation occurred not in the state of residence, but in a different Member State. Consequently, in such a situation what sort of powers has the DPA of local residence, if it is not competent according to Article 51?
7. The introductory explanation about the functioning of the OSS provided by Germany proved to be very useful in understanding the essence of the procedure. Therefore Hungary would be very grateful to have a similar explanation concerning Article 74 (1) and in particular its relation to the other elements of the legal redress system. Is it a correct interpretation that the data subject has the right to judicial remedy against a decision of another Member State's DPA, brought before the court of his/her habitual residence?

ONE-STOP-SHOP MECHANISM (document 5882/2/14)

Article 51a

Competence for acting as lead supervisory authority

1. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State **or the processing substantially affects or is likely to affect substantially data subjects in more than one Member State**, the supervisory authority for the main establishment shall act as lead supervisory authority and shall be competent to decide on measures applying the powers conferred on it in accordance with the cooperation procedure foreseen in Articles 54a and 54b.
2. ~~Where the processing of personal data takes place in the context of the activities of one establishment of a controller or processor in the Union and the processing substantially affects or is likely to affect substantially data subjects in more than one Member State, the supervisory authority of that establishment shall act as lead authority and shall be competent to decide on measures applying the powers conferred on it in accordance with Articles 54a and 54b.~~
3. Paragraph 1 shall not apply where the subject matter concerns only processing carried out in a single Member State and involving only data subjects in that Member State.
4. **The paragraphs 1 and 2 of** this article shall not apply where the processing is carried out by public authorities and bodies of a Member State. The only supervisory authority competent to exercise the powers conferred on it in accordance with this Regulation regarding a Member State's public authorities and bodies shall be the supervisory authority of that Member State.

Article 76

Representation of data subjects

1. The data subject shall have the right to mandate a body, organisation or association, which has been properly constituted according to the law of a Member State and whose statutory objectives include the protection of data subjects' rights and freedoms with regard to the protection of their personal data, to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf.
- 1a. ~~Independently of a data subject's mandate or complaint, any body, organisation or association referred to in paragraph 1 shall have the right to lodge a complaint with the supervisory authority competent in accordance with Article 51 if it has reasons to consider that a personal data breach referred to in Article 32(1) has occurred and Article 32(3) does not apply.~~
2. (...)
3. (...)
4. (...)
5. (...)

CONTRIBUTION OF THE CLS:

Effective judicial protection of data subjects' fundamental rights in the context of the envisaged "one-stop shop" mechanism (document: 18031/13)

PL comments :

- The opinion of EDPS on the one-stop-shop presented in a letter issued on 14th February 2014 should be taken into account while deciding on the future shape of the one-stop-shop model

- Opinion of the CLS does not relate to the current legal situation and the situation of data subjects under the provisions of Directive 95/46. In our view the solutions proposed by draft Regulation are more advantageous for the data subjects than the situation under current Directive, where the data subject may only complain to the DPA which is competent due to the establishment or location of equipment of the controller or processor concerned, what creates a situation in which data subject must seek protection of their rights in a foreign legal system and in a foreign language. The draft regulation gives data subject the right to lodge a complaint with the supervisory authority in any Member State (Article 73 par. 1) as well as the right to bring legal proceedings against controller or processor before the courts of the Member States where the data subject has his or her habitual residence (Article 75 par. 2), which is a major improvement of data protection rights of individuals compared to the Directive 95/46.
- The competence of a lead authority is not exclusive, and its decision is preceded by the procedure of cooperation and consistency procedure, including the right of the DPAs concerned to object to the draft measure (Article 54a par. 3 and Article 54b par. 4). Decision-making in matters covered by the mechanism of one-stop -shop therefore takes place with the full involvement and cooperation of the DPAs concerned.
- In fact, the one-stop-shop principle would apply in a limited number of 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 controller or processor is established in more than one Member State or the processing substantially affects or is likely to affect substantially data subjects in more than one Member State (in accordance with art. 51a) . The one-stop-shop will therefore not be a standard mechanism for the implementation of powers of the DPAs.

- Poland supports a strong position of the European Data Protection Board – it is a vital element of an effective consistency mechanism. We do not oppose giving the EDPB legal personality and the power to adopt legally binding decisions in the consistency mechanism. The CLS proposal to have the EDPB hear direct complaints is however unrealistic. Neither the Board nor the General Court would be able to handle such a case load. This idea also doesn't solve the problem of the “duality” of proceedings – civil and administrative. This solution would not ensure the better “proximity” of the legal proceedings to the citizens - all proceedings would be brought in Brussels/ Luxembourg, which would not be beneficial not only from the point of view of the data subjects but also for the entrepreneurs.
- Furthermore, since the decision of the EDPB would be subject only to judicial review by the CJEU (i.e. only one instance) there will be no possibility to appeal its final judgment. This may be in violation of the right to a judicial appeal guaranteed by the Polish Constitution.

Comments on the German proposal

Poland's primary reservation towards the German Proposal is that it constitutes a reversal of the one-stop-shop principle. According to the one-stop-shop rule, when the processing of personal data takes place in more than one Member State, only the supervisory authority of the Member State, where the main establishment of the controller or processor is located, is responsible for taking legally binding decisions imposed on the controller or processor, which would be then enforceable in all the Member States concerned. The process of decision-making by the main establishment authority should be accompanied by the close cooperation with the concerned DPAs, which according to Poland, is sufficiently provided in Presidency's document (5882/3/14 REV 3).

The procedure of the decision-making by DPAs, as proposed in the German document (6637/14), seems to us complex, overly bureaucratic and time-consuming. We consider it as a kind of an extra degree of consultation between DPAs prior to the mechanism of compliance and co-operation.

In the Union-wide compliance procedure in Poland's opinion, DPAs from all EU Member States are unduly involved in the decision-making process. The possible number of cases in the Union-wide compliance procedure may lead to excessive workload for the DPAs and the lack of real possibilities of handling them.

In this respect we would like to seek the opinion of the Article 29 working party and the EDPS on the feasibility of such a procedure. In our view the whole procedure would be lengthy and, in almost every case, engaging the EDPB, as it is sufficient that only one DPA objects, so that the case is transferred to the EDPB under the co-operation procedure (Article 58).

As for the Union-wide non-compliance procedure Poland remains opposed to the idea of giving each DPA the possibility of issuing a Union-wide draft non-compliance decision, which is a solution contrary to the one-stop-shop principle. The decision concerning the processing activities of the controller or processor in the EU shall be issued by the DPA which is competent for these activities (the one in the Member State in which a business has its main establishment).

Implementation of the union-wide non-compliance procedure, as proposed in the document 6637/14, will lead to a situation in which data controllers operating in more than one Member State will face the risk of being involved in proceedings regarding various matters in different Member States. As proposals for a decision will be issued by various supervisory authorities from different Member States, it may create the risk of reaching different decisions in similar cases. The DPAs may also refuse to follow an opinion of the EDPB which is non-binding (Art. 58a par. 8-9).

The union-wide non-compliance procedure will not provide uniformity in application of the law, because it seems that in the German proposal (according to art. 57 par. 7), a decision will be binding only in the territory of those Member States whose supervisory authorities have given their consent for the decision to be binding. This will lead to legal uncertainty and differences in law enforcement in individual Member States.

What is more, it seems that the controllers can only appeal to the court in the Member State where the supervisory authority has initiated the procedure for non-compliance and not to the court in the Member State, where the business has its main establishment. This would be a major impediment to business and will not bring any improvements to the situation which we have under the Directive 46/95.

The solution proposed by the German delegation in the case of the union-wide non-compliance procedure, resulting in the lack of legal clarity and harmonisation would lead to deterioration of the conditions for business operating in the EU. The concept of the risk-based approach, on which we agreed under the Irish Presidency, should be applied also in the case of procedure of the decision making by the DPAs in transnational cases.

In Poland's opinion the German proposal does not solve the proximity issue because any decisions of the EDPB could only be challenged before the European Court of Justice (ECJ). As for a data subject and for a controller or a processor it would mean the necessity to seek judicial redress in Luxembourg in almost all of the cases as according to Poland vast majority of the compliance procedures would end up with the decision taken by the EDPB. This solution seems to be unfeasible at the moment because of the limited capacity of the ECJ to deal with such an amount of cases and creates the risk of the unacceptably long legal proceedings.

As for the role of the EDPB, Poland sees the added value in the EDPB having legal personality and handing down binding decisions, as it would ensure harmonisation and consistency of the Regulation enforcement in the EU. We are concerned however about the feasibility of the EDPB taking decision in each case, as it would require the increased staff and resources to ensure its efficiency. Therefore, the role of the EDPB should be limited to exceptional cases where the matter cannot be resolved through consistent cooperation of supervisory authorities as in the Presidency's document (5882/3/14 REV 3).

| <u>Presidency proposal</u> | <u>DE Proposal</u> | <u>comments</u> |
|----------------------------|--|---|
| | <p style="text-align: center;"><u>Article 34a</u> <u>Decision on Compliance</u></p> <p><u>1. Controllers, processors, joint controllers or group of undertakings which have their main establishment in the Union or have designated an representative pursuant to Art. 25 (applicants) may on request obtain a Union-wide compliance decision in trans-border cases from the competent supervisory authority, in order to ensure the compliance of data processing with this Regulation.</u></p> <p><u>2. In order to obtain a compliance decision the applicant shall make a request to the supervisory authority. In the request the applicant must describe and explain</u></p> <p><u>(a) the controller, processor, joint controllers or group of undertakings to which the decision shall apply,</u></p> <p><u>(b) the category of data processing practiced or planned,</u></p> <p><u>(c) the concrete concept that the data processing is based on and that is to be examined in the compliance procedure,</u></p> | <p>Comparison between the Presidency’s proposal on one-stop-shop and the German alternative proposal is on several instances quite a difficult task since the proposals are substantially two completely different one-stop-shop concepts.</p> <p>While the presidency’s proposal builds on the initial Commission proposal, keeping the same architecture but trying to improve or find solutions for the problems of lengthy, complex and remote from citizen’s procedure, the architecture of the German proposal is completely new, and builds on two complementary procedures: <i>first</i> is the procedure to obtain an EU-wide decision on the compliance of data processing, a procedure intended to safeguard the interests of legal certainty for <u>businesses</u> that their processing is in compliance with EU law, and <i>second</i> is a procedure for a decision on the non-compliance of data processing which is intended to safeguard interests of <u>data subjects</u> and <u>data protection</u> authority when they believe that certain data processing by controllers is not compliant with the EU law.</p> |

| | | |
|--|---|---|
| | <p><u>(d) the legal basis of the data processing pursuant to Article 6 and the measures to protect the data subject pursuant to this Regulation.</u></p> <p><u>(e) the data protection impact assessment as provided for in Article 33 indicating that the processing is likely to present a high degree of specific risks.</u></p> <p><u>(f) a reasonable interest</u></p> <p><u>aa) in a compliance decision, for example in the case of the introduction of new data processing or a processing for which no established practice or, clear opinion of the supervisory authority exists and</u></p> <p><u>bb) in a Union-wide decision, notably the importance of the data processing for a substantial number of data subjects concerned in more than one Member State or the existence of establishments in more than one Member State.</u></p> | <p>Article 34a of the German proposal is tightly connected to Article 56 and the first of the two complementary procedures – the so called Union-Wide Compliance Procedure. It is a non-compulsory procedure which gives businesses the opportunity not only to request a confirmation of the indication of the “lead” Supervisory Authority - or in other words their “one-stop-shop” - (as is the case in the Presidency’s proposal of Article 51b) but it goes a step further in providing businesses with an option to also get a confirmation on the compliance of their data processing activities (the interest of legal certainty).</p> |
|--|---|---|

| | | |
|---|--|--|
| <p style="text-align: center;"><i>Article 51</i> Competence</p> <p>1. Each supervisory authority shall (...) be competent <u>on the territory of its own Member State</u> to (...) perform the duties and to exercise the powers conferred on it in accordance with this Regulation, <u>without prejudice to Article 51a.</u></p> <p>a) (...)</p> <p>b) (...)</p> <p>c) (...)</p> <p>1a. (...)</p> <p>1b. (...)</p> <p>1c. (...)</p> <p>2. (...)</p> <p>2a. (...)</p> <p>2b. (...)</p> <p>3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.</p> | <p style="text-align: center;"><i>Article 51</i> Competence</p> <p>1. Each supervisory authority shall be competent <u>to monitor the application of this Regulation and</u> exercise the powers conferred on it in accordance with this Regulation regarding each of the following:</p> <p>a) processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State;</p> <p>b) processing <u>which is related to the offering of goods and services to data subjects on its own Member State by controllers not established in its own Member State;</u> or</p> <p>c) processing referred to in paragraph 2 of Article 3 which is related to data subjects on its territory by a controller established outside of the European Union.</p> | <p>The question of <u>competent authority</u>, especially in cases where controller has establishments in several Member States:</p> <p style="text-align: center;"><i>A) Presidency proposal:</i></p> <ul style="list-style-type: none"> • Situation 1: Single MS establishment (Article 51): Competent authority is the Supervisory Authority of the MS of the establishment (the so called “local cases” where the problem of having only one-stop in one Member state does not even arise) • Situation 2: Multi MS establishments (1 paragraph of Article 51a): The <u>lead authority</u> is the <u>Supervisory Authority of the main establishment</u> (the main establishment rule = 1. The place of <i>central administration</i> unless 2. <i>main data processing decisions</i> are taken in another MS and 3. If central administration and decisions are taken outside EU, the MS where <i>main processing activities</i> take place). <p>The “main establishment” authority is not solely and fully competent for supervision of the data processing activities of controller but (only) has a leading role (lead authority) in the co-operation process between Supervisory authority of all MS concerned.</p> |
|---|--|--|

| | | |
|--|---|--|
| <p style="text-align: center;"><i>Article 51a</i></p> <p><i>Competence for acting as lead supervisory authority</i></p> <p><u>1. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State, the supervisory authority for the main establishment shall act as lead supervisory authority and shall be competent to decide on measures applying the powers conferred on it in accordance with the cooperation procedure foreseen in Articles 54a and 54b.</u></p> <p><u>2. Where the processing of personal data takes place in the context of the activities of one establishment of a controller or processor in the Union and the processing substantially affects or is likely to affect substantially data subjects in more than one Member State, the supervisory authority of that establishment shall act as lead authority and shall be competent to decide on measures applying the powers conferred on it in accordance with Articles 54a and 54b.</u></p> | <p>1a. The only supervisory authority competent to perform the duties and exercise the powers conferred on it in accordance with this Regulation regarding a Member State's public authorities and bodies shall be the supervisory authority established in that Member State.</p> <p><u>2. Each supervisory authority may become lead authority of a Union-wide procedure to approve or disapprove the lawfulness of a data processing:</u></p> <p><u>(a) The competent lead authority of a compliance procedure pursuant to Article 56 shall be the supervisory authority of the Member State in which the controller or the processor filing the request (the applicant) has its main establishment according to its articles of association or, if it does not have a main establishment within the Union, its representative pursuant to Article 25.</u></p> <p><u>(b) The competent lead authority of a non-compliance procedure pursuant to Article 57 shall be the supervisory authority that considers such procedure necessary or where a data subject has lodged a complaint.</u></p> | <ul style="list-style-type: none"> • Situation 3: Processing takes place in ONE establishment and the processing substantially affects data subjects in MORE THAN ONE MS. <p>The lead authority is the Supervisory Authority of the Member State where the establishment is.</p> <p style="text-align: center;"><u>B) German proposal – applying the same 3 situations to the German proposal:</u></p> <ul style="list-style-type: none"> • Situation 1: Single MS establishment (Article 51): same as in the Presidency proposal. • Situation 2: Multi MS establishments (2 paragraph of Article 51, (a) and (b)). <p>For the question of the competent/lead authority the German proposal differentiates between two different complementary procedures:</p> <p>a) <u>For the Union-Wide Compliance procedure</u> (a procedure intended to safeguard the interests of legal certainty for <i>businesses</i> that their processing is in compliance with EU law): the <u>lead authority</u> is the <u>Supervisory Authority of the main establishment</u>, or if it doesn't have its main establishment in the EU <u>of its representative (Article 51(2)(a)).</u></p> |
|--|---|--|

| | | |
|--|--|--|
| <p>3. <u>Paragraph 1 shall not apply where the subject matter concerns only processing carried out in a single Member State and involving only data subjects in that Member State.</u></p> | | <p>b) <u>For the Union-Wide Non-Compliance procedure</u> (a procedure intended to safeguard interests of <i>data subjects</i> and <i>data protection</i> authority when they believe that certain data processing by controllers is not compliant with the EU law): the lead authority is the <u>supervisory authority that considers such procedure necessary or where a data subject has lodged a complaint (Article 51(2)(b)).</u></p> |
| <p>4. <u>This article shall not apply where the processing is carried out by public authorities and bodies of a Member State.</u> The only supervisory authority competent to exercise the powers conferred on it in accordance with this Regulation regarding a Member State's public authorities and bodies shall be the supervisory authority of that Member State.</p> | | <p>• Situation 3: Processing in ONE establishment but significantly effects Data Subjects in SEVERAL MS: The German proposal does not explicitly address this situation, however it is interesting to play out this option how it would work out in practice:</p> <p>a) In the case of Non-Compliance procedure the Data Subject can file a complaint in its own Member State (even though the establishment and data processing are taking place in another MS) and the lead authority is the Supervisory Authority of the MS where DS has lodged its complaint – so the proximity requirement as regards DS is satisfied. As for the Supervisory Authority any Supervisory authority that considers non-compliance procedure necessary can initiate the non-compliance procedure and by doing so becomes a lead authority. There is however a problem of “proximity” in relation to the Supervisory Authority in cases where the lead supervisory authority is not the one of the</p> |

| | | |
|---|--|---|
| <p style="text-align: center;"><i>Article 51b¹</i></p> <p style="text-align: center;"><u>Identification of the supervisory authority competent for the main establishment</u></p> <p>1. Any controller or processor may indicate to the supervisory authority of the Member State in which it considers that its main establishment is located the scope of its processing activities and ask it for confirmation that it is the <u>lead supervisory</u> authority referred to in paragraphs <u>1 and 2</u> of Article 51a. The authority shall communicate its reply to the other supervisory authorities concerned. <u>These replies may be made public by means of a public register maintained by the secretariat of the European Data Protection Board.</u></p> | | <p>establishment where the processing solely takes place but rather the supervisory authority of a MS whose citizens are severely affected by the data processing. In these cases it will be practically impossible for the SA who initiated the non-compliance procedure to actually effectively exercise its role as a lead authority (namely an obligation to prepare a non-compliance decision from Article 57(2)) since it will be impossible for this authority to exercise investigative, corrective etc. powers on the territory of another supervisory authority! This is a shortcoming that would need to be addressed if the German proposal is to be adopted.</p> |
|---|--|---|

¹ Moved from Article 57a.

| | | |
|--|--|---|
| <p>2. Where there are conflicting views between the supervisory authorities concerned on which supervisory authority is (...) that for the main establishment, any of the supervisory authorities concerned may refer the matter to the European Data Protection Board. The European Data Protection Board shall issue an opinion on the identification of the supervisory authority for the main establishment in accordance with Article 58.</p> | | <p>b) In the case of the compliance procedure: For the controller the competent authority will be the Supervisory Authority of its establishment. For DS and SA the compliance procedure does not apply since it is intended only to safeguard the interests of controllers.</p> |
| <p style="text-align: center;"><i>Article 52</i> Duties</p> <p>1. Without prejudice to other duties set out under this Regulation, each supervisory authority shall on its territory:</p> <p>(a) monitor and enforce the application of this Regulation;</p> <p>(aa) promote public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention;</p> <p>(ab) provide information to the national parliament, the government or other political institution as well as the public on any issue related to the protection of personal data</p> <p>(ac) promote the awareness of controllers and processors of their obligations under this Regulation;</p> | <p style="text-align: center;"><i>Article 52</i> Duties</p> <p>1. Without prejudice to other duties set out under this Regulation, each supervisory authority shall on its territory:</p> <p>(a) monitor and enforce the application of this Regulation;</p> <p>(aa) promote public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention;</p> <p>(ab) inform the national parliament, the government or other political institution as well as the public on any issue related to the protection of personal data;</p> <p>(ac) promote the awareness of controllers and processors of their obligations under this Regulation;</p> | |

| | | |
|---|--|--|
| <p>(ad) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end;.</p> <p>(b) deal with complaints lodged by a data subject, or body, organisation or association representing a data subject in accordance with Article 73 , and investigate, to the extent appropriate, the subject matter of the complaint and inform the data subject or the body, organisation or association of the progress and the outcome of the investigation within a reasonable period , in particular if further investigation or coordination with another supervisory authority is necessary;</p> <p>(c) share information with and provide mutual assistance to other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;</p> <p>(d) conduct investigations on the application of this Regulation either on its own initiative or on the basis of a information received from another supervisory authority or other public authority;</p> | <p>(ad) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.</p> <p>(b) deal with complaints lodged by a data subject, or body, organisation or association representing a data subject in accordance with Article 56a and 57a, and investigate, to the extent appropriate, the subject matter of the complaint and inform the data subject or the body, organisation or association of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;</p> <p>(c) share information with and provide mutual assistance to other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;</p> <p>(d) conduct investigations on the application of this Regulation either on its own initiative or on the basis of a information received from another supervisory or other public authority;</p> | |
|---|--|--|

| | | |
|---|---|--|
| <p>(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;</p> <p>(f) (...);</p> <p>(fa) (...);</p> <p>(g) (...);</p> <p>(ga) (...);</p> <p>(gb) (...);</p> <p>(gc) (...);</p> <p>(gd) (...);</p> <p>(h) (...);</p> <p>(ha) (...);</p> <p>(hb) (...);</p> <p>(i) (...);</p> <p>(j) contribute to the activities of the European Data Protection Board;</p> <p>(k) issue opinions as well as fulfil any other duties related to the protection of personal data.</p> <p>2. (...).</p> <p>3. (...).</p> | <p>(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;</p> <p>(j) contribute to the activities of the European Data Protection Board;</p> <p>(k) issue opinions as well as fulfil any other duties related to the protection of personal data;</p> <p><u>(l) make a decision on the compliance or non-compliance of data processing activities or planned data processing activities with this Regulation pursuant to Article 56 and Article 57.</u></p> | |
|---|---|--|

| | | |
|--|---|--|
| <p>4. Each supervisory authority shall enable the submission of complaints referred to in point (b) of paragraph 1, by measures which can be completed electronically, such as providing a complaint submission form, without excluding other means of communication.</p> | <p>4. Each supervisory authority shall enable the submission of complaints referred to in point (b) of paragraph 1, by measures which can be completed electronically, such as providing a complaint submission form, without excluding other means of communication.</p> | |
| <p>5. The performance of the duties of each supervisory authority shall be free of charge for the data subject and for the data protection officer.</p> | <p>5. The performance of the duties of each supervisory authority shall be free of charge for the data subject and for the data protection officer.</p> | |
| <p>6. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may refuse to act on the request . The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.</p> | <p>6. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.</p> | |

| | | |
|--|--|---|
| | <p style="text-align: center;"><u>Article 52a</u></p> <p style="text-align: center;"><u>Cooperation and mutual assistance between supervisory authorities</u></p> <p><u>1. The supervisory authorities of the Member States shall provide each other with all useful information, analysis and mutual assistance on questions of fact or law in order to implement this Regulation in a consistent manner.</u></p> <p><u>2. The lead authority shall, without undue delay, provide the other competent supervisory authorities with all relevant information and analyses obtained while performing its duties. Any competent supervisory authority may also request relevant information and analyses from the lead authority.</u></p> <p><u>3. The European Data Protection Board shall be used to facilitate the cooperation and the exchange of information. Therefore the European Data Protection Board could establish a situation centre with liaison officers from the supervisory authorities of the Member States.</u></p> <p><u>4. For the purposes of applying the provisions of this article, the supervisory authorities and the European Data Protection Board shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.</u></p> | <p>The German proposal in general strengthens the role of EDPB which is an integral part of consistency mechanism (in the German proposal the EDPB is entrusted with legal personality, can issue legally binding opinions and its decision can be appealed before the General Court).</p> <p>Furthermore when it comes to mutual assistance the German proposal also gives EDPB a central role (paragraph 3), whereas in the presidency’s proposal the role of EDPB is more or less marginal, and only comes up front in cases where supervisory authorities do not respond to the mutual assistance requests. While stronger role of EDPB in cases of mutual assistance might not really be needed (as it suffices that only Supervisory Authorities concerned are actually involved in the mutual assistance proceeding in order not to impose too much burden on EDPB), the envisaged situation centre in paragraph 3 depending on its structure might be an acceptable idea (but not necessary).</p> |
|--|--|---|

| <p style="text-align: center;"><i>Article 53</i></p> <p style="text-align: center;">Powers</p> | <p style="text-align: center;"><i>Article 53</i></p> <p style="text-align: center;">Powers</p> | |
|--|--|--|
| <p>1. Each Member State shall provide by law that its supervisory authority shall have at least the following investigative powers:</p> <p>(a) to order the controller and the processor , and, where applicable, the representative to provide any information it requires for the performance of its duties;</p> <p>(aa) to carry out data protection audits ;</p> <p>(b) (...)</p> <p>(c) (...)</p> <p>(d) to notify the controller or the processor of an alleged infringement of this Regulation (...);</p> <p>(da) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its duties;</p> <p>(db) to obtain access to any premises of the controller and the processor , including to any data processing equipment and means.</p> <p>1a. (...).</p> | <p>1. Each Member State shall provide by law that its supervisory authority shall have at least the following monitoring powers:</p> <p>(a) to order the controller and the processor, and, where applicable, the representative to provide any information it requires for the performance of its duties;</p> <p>(b) to carry out data protection audits;</p> <p>(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights provided by this Regulation;</p> <p>(d) to notify the controller or the processor of an alleged infringement of this Regulation, and where appropriate, order the controller or the processor to remedy that infringement;</p> <p>1a. Each Member State shall provide by law that its supervisory authority shall have at least the following investigatory powers:</p> <p>(a) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its duties;</p> <p>(b) to obtain access to any premises of the controller and the processor , including to any data processing equipment and means.</p> | |

| | | |
|---|--|--|
| <p>1b. Each Member State shall provide by law that its supervisory authority shall have the following corrective powers:</p> <p>(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;</p> <p>(b) to issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation;</p> <p>(c) (...);</p> <p>(ca) <u>to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;</u></p> <p>(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; inter alia by carrying out a data protection audit or by ordering the rectification, restriction or erasure of data pursuant to Articles 16, 17a and 17 and the notification of such actions to recipients to whom the data have been disclosed pursuant to Articles 17(2a) and 17b;</p> | <p>1b. Each Member State shall provide by law that its supervisory authority shall have the following corrective powers:</p> <p>(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;</p> <p>(b) to issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation;</p> <p>(c) (...);</p> <p>(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; inter alia by carrying out a data protection audit or by ordering the rectification, restriction or erasure of data pursuant to Articles 16, 17a and 17 and the notification of such actions to recipients to whom the data have been disclosed pursuant to Articles 17(2a) and 17b;</p> | |
|---|--|--|

| | | |
|---|---|--|
| <p>(e) to impose a temporary or definitive limitation on processing ;</p> <p>(f) to order the suspension of data flows to a recipient in a third country or to an international organisation ;</p> <p>(g) to impose an administrative fine pursuant to Articles 79 and 79a, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.</p> <p>1c. Each Member State shall provide by law that its supervisory authority shall have the following authorisation powers:</p> <p>(a) advise the controller in accordance with the prior consultation procedure referred to in Article 34,</p> <p>(b) authorise standard data protection clauses referred to in point (c) of Article 42(2);</p> <p>(c) authorise contractual clauses referred to in point (d) of Article 42(2);</p> <p>(d) approve binding corporate rules pursuant to Article 43.</p> <p>2. The procedure for exercising the powers referred to in paragraphs 1, 1a, 1b and 1c shall be laid down in Member State law. (...)¹</p> | <p>(e) to impose a temporary or definitive limitation on processing;</p> <p>(f) to order the suspension of data flows to a recipient in a third country or to an international organisation;</p> <p>(g) to impose an administrative fine pursuant to Articles 79 and 79a, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.</p> <p>1c. Each Member State shall provide by law that its supervisory authority shall have the following authorisation powers:</p> <p>(a) give advice in accordance with the prior consultation procedure referred to in Article 34,</p> <p><u>(b) make a decision on compliance pursuant to Article 34a ;</u></p> <p>(c) authorise standard data protection clauses referred to in point (c) of Article 42(2);</p> <p>(d) authorise contractual clauses referred to in point (d) of Article 42(2);</p> <p>(e) approve binding corporate rules pursuant to Article 43.</p> <p>2. The procedure for exercising the powers referred to in paragraphs (1), (1a), (1b) and (1c) shall be laid down in Member State law. The exercise of those powers shall be subject to appropriate procedural safeguards, including effective judicial remedy and due process, set out in Union and Member State law.</p> | |
|---|---|--|

¹ Moved to new Article 53a.

| | | |
|---|---|--|
| <p>3. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities or to commence or engage otherwise in legal proceedings , in order to enforce the provisions of this Regulation.</p> <p>4. (...)</p> <p>5. (...)</p> | <p>3. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities or to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.</p> | |
| <p style="text-align: center;"><i>Article 53a</i></p> <p><u>Exercise of powers by the supervisory authority</u></p> <p>1. <u>The exercise of the powers conferred on the supervisory authority pursuant to Article 53 shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law.</u></p> <p>2. <u>When exercising the powers referred to in Article 53, each supervisory authority shall act impartially, fairly and within a reasonable time. In particular each measure shall:</u></p> <p><u>(a) be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case and legitimate interests of the persons concerned;</u></p> | | |

| | | |
|--|--|--|
| <p><u>(b) respect the right of every person to be heard, before any individual measure which would affect him or her adversely is taken;</u></p> <p><u>(c) avoid superfluous costs and excessive inconveniences for the persons concerned;</u></p> <p><u>(d) be taken without undue delay.</u></p> <p><u>3. Each legally binding measure of the supervisory authority exercising the powers referred to in Article 53 shall be in writing and:</u></p> <p><u>(a) be clear and unambiguous;</u></p> <p><u>(b) indicate the supervisory authority;</u></p> <p><u>(c) indicate the time of issuance of the measure;</u></p> <p><u>(d) bear the signature of the head or a member of the supervisory authority of a person authorised by him or her;</u></p> <p><u>(e) give the reasons for the measure;</u></p> <p><u>(f) refer to the right of an effective remedy and give contact details of the competent court, indicating the form and time limits for such remedy.</u></p> | | |
|--|--|--|

| | | |
|---|---|--|
| <p style="text-align: center;">CHAPTER VII CO-OPERATION AND CONSISTENCY SECTION 1 CO-OPERATION</p> | <p style="text-align: center;">CHAPTER VII CONSISTENCY SECTION <u>I</u> CONSISTENCY <u>MECHANISMS</u> <i>Section 1 (Co-operation) in the German proposal is deleted/merged with consistency section.</i></p> | |
| <p style="text-align: center;"><i>Article 54a</i></p> <p><i>Cooperation between the lead supervisory authority and other supervisory authorities concerned</i></p> <p>1. <u>In the cases referred to in paragraphs 1 and 2 of Article 51a, (...) the lead supervisory authority (...) shall cooperate with the supervisory authorities concerned by the processing in question in accordance with this article and with Article 54b in an endeavour to reach consensus (...). A supervisory authority is concerned by the processing, where there is an establishment of the controller or processor in its Member State or where a data subject residing in this Member State is likely to be substantially affected by the processing.</u></p> | <p style="text-align: center;"><i>Article 55</i></p> <p style="text-align: center;"><u>Consistency mechanisms</u></p> <p>1. <u>For the purpose set out in Article 46 (1a), the supervisory authorities shall co-operate with each other through the consistency mechanisms as set out in this section. Consistency mechanisms are</u></p> <p><u>(a) the Union-wide compliance procedure (Article 56),</u></p> <p><u>(b) the Union-wide non-compliance procedure (Article 57),</u></p> <p><u>(c) the co-operation procedure (Article 58).</u></p> | <p>On this point the presidency's proposal and the German proposal are substantially two completely different one-stop-shop concepts, given their different concepts of who is the competent lead authority.</p> <p style="text-align: center;"><u>a) The Architecture of the German proposal</u></p> <p>There are two complementary procedures:</p> <p>1. the procedure to obtain an <i>EU-wide decision on the compliance of data processing (Article 56)</i>: the procedure is of a voluntary basis and allows each controller to obtain an EU-wide decision finding its data processing compliant with the EU law as a way of protecting his interests for legal certainty.</p> |

| | | |
|--|---|---|
| <p><u>1a. Where, in a case referred to in paragraph 1 or 2 of Article 51a, a supervisory authority concerned considers a measure intended to produce legal effects by applying the powers referred to in paragraphs 1, 1b and 1c of Article 53 as appropriate in view of the processing in question, it shall refer the matter to the lead supervisory authority.</u></p> <p>2. (...) <u>The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the supervisory authorities concerned and shall, without prejudice to Article 54b:</u></p> <p>a) (...);</p> <p>b) submit the draft <u>of a measure referred to in paragraph 1a</u> to all supervisory authorities (...)concerned <u>for their opinion</u>;</p> <p>c) take utmost account of the views of the supervisory authorities (...);</p> <p><u>(ca) adopt and notify the measure referred to in paragraph 1a to the controller or processor.</u></p> | <p style="text-align: center;"><u>Article 56</u></p> <p style="text-align: center;"><u>Union-wide Compliance Procedure</u></p> <p><u>1. Controllers or processors which have their main establishment in the Union or have designated an representative pursuant to Art. 25 may use the Union-wide compliance procedure to obtain a Union-wide legally binding decision as to whether their data processing complies with this Regulation in the following cases:</u></p> <p><u>(a) decisions on compliance pursuant to Article 34a,</u></p> <p><u>(b) draft codes of conduct or amendments or extensions to a code of conduct pursuant to Article 38(2),</u></p> <p><u>(c) standard data protection clauses pursuant to point (c) of Article 42(2),</u></p> <p><u>(d) contractual clauses between the controller or processor and the recipient of the data pursuant to point (d) of Article 42(2),</u></p> <p><u>(e) binding corporate rules pursuant to Article 43</u></p> | <p>According to the procedure the controller needs to file an application (Article 34a) with the lead supervising authority which is solely responsible for all issues related to a positive EU-wide compliance decision. Lead authorities are the authorities in those Member States where the business has its main establishment or representatives in the EU (the same rule as in the Presidency’s one-stop-shop proposal). The lead authority must then consult national supervisory authorities through the EDPB. If the lead authority wants to approve the application of the businesses based on a complete request pursuant to Art. 34a, it must draft a compliance decision within two months. The draft is distributed to the supervisory authorities involved via the EDPB. If they do not object to the lead authority's draft within six weeks they are bound by that decision (meaning this decision can also be subject of judicial review before the national courts of the Supervisory</p> |
|--|---|---|

| | | |
|--|--|---|
| <p>2a. <u>The lead supervisory authority may request/ask at any time other concerned supervisory authorities to provide mutual assistance pursuant to Article 55, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.</u></p> <p>3. Where any of the supervisory authorities <u>concerned</u> objects, within a period of four weeks after having been consulted under paragraphs 1 or 2, to the draft measure <u>referred to in point (b) of paragraph 2</u>, this authority <u>shall</u> submit the matter to the consistency mechanism referred to in Article 57. Where a supervisory authority concerned has not objected within this period, it is deemed to be in agreement with the draft measure.</p> <p>4. (...)</p> <p>4a. (...)</p> <p>4b. <u>Where a concerned supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 61 shall apply.</u></p> | <p><u>2. The Union-wide compliance procedure shall be initiated at the request of a controller, processor, joint controller or group of undertakings(applicant) or any national supervisory authority.</u></p> <p><u>3. The request shall be filed with the lead authority as referred to in Article 51 (2) a.</u></p> <p><u>4. The lead authority shall forward without delay any request in due form to the European Data Protection Board. The European Data Protection Board shall forward the request to the supervisory authorities of the other Member States.</u></p> | <p>Authorities concerned. If one Member State objects to the draft decision of the lead authority, any national supervisory authority, the European Commission or the EDPB may launch the cooperation procedure pursuant to Art. 58. The cooperation procedure is concluded by a binding decision of the EDPB (because it is binding and EDPB has a legal personality (Article 64 of the German proposal) this decision can also be subject to judicial review before the General Court). The decision finding process within the EDPB is a voting procedure of the Member States' data protection supervisory authorities. If less than 1/3 of the Member States objected to the draft, the majority decision should be binding for all Member States. If more than 1/3 of the Member States objected to the draft, the EDPB may prepare a new draft which reflects the concerns of the Member States. If the EDPB draft is rejected as well, EDPB communicates the results of the cooperation</p> |
|--|--|---|

| | | |
|--|---|---|
| <p>5. The supervisory authority of the main establishment of the controller or processor and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.</p> <p style="text-align: center;"><i>Article 54b</i></p> <p style="text-align: center;">Cooperation on complaints lodged to a supervisory authority</p> <p>1. <u>Where a complaint has been lodged to a supervisory authority other than the one which is competent for the matter in accordance with Article 51(1) or acts as a lead supervisory authority pursuant to paragraph 1 or 2 of Article 51a, that supervisory authority shall, without prejudice to point (b) of Article 52(1), refer the matter to the lead supervisory authority.</u></p> | <p><u>5. The lead authority shall make a decision on the request within two months of receiving it in due form:</u></p> <p><u>(a) If the lead authority considers that the data processing of the applicant complies with applicable data protection law, it shall draft a compliance decision.</u></p> <p><u>(b) If the lead authority considers that the data processing of the applicant does not comply with the applicable data protection law, it shall reject the request for a compliance decision. This rejection is legally binding in the territory of the Member State of the lead authority. The lead authority shall decide after due consideration whether to initiate a non-compliance procedure pursuant to Article 57.</u></p> | <p>procedure to the business. Regardless of the competences of the supervisory authorities for the application of this Regulation on the territory of its own Member State, the EDPB may decide whether to seek solutions for the consistent application of this Regulation by issuing general guidelines or other non-binding recommendations on the questions raised by the compliance procedure.</p> |
|--|---|---|

| | | |
|---|---|---|
| <p><u>2. In a case referred to in paragraph 1 or 2 of Article 51a the supervisory authority to which the complaint has been lodged, where the subject matter of the complaint concerns only processing activities of an establishment of the controller or processor in one single Member State and the matter does not affect data subjects in another Member State, the supervisory authority to which the complaint has been lodged may, where appropriate, seek an amicable settlement of the complaint. Where such amicable settlement cannot be reached or where such an amicable settlement would not be appropriate, the supervisory authority to which the complaint has been lodged shall refer the matter and the result of its related investigations to the lead supervisory authority, which shall act pursuant to points (b) and (c) of Article 54a(2).</u></p> | <p><u>6. If the lead authority drafts a compliance decision pursuant to paragraph 6a it shall forward it without delay in a standardized way to the European Data Protection Board. The European Data Protection Board shall forward the draft compliance decision in a standardized way. The supervisory authorities shall submit comments and/or an objection in accordance with paragraph 7 within six weeks.</u></p> | <p>2. the procedure for a <i>decision on the non-compliance (Article 57)</i> in which any data subject and data protection supervisory authority is allowed to initiate a procedure to establish non-compliance of data processing, particularly on the request of a citizen. The supervisory authority notifies a business of its intention to initiate a procedure and makes appropriate recommendations. If the business does not comply with the recommendations within one month, the supervisory authority initiates the EU-wide non-compliance procedure. In this case, the business may apply for a EU-wide compliance procedure. Initiating a compliance procedure suspends the non-compliance procedure. The authority may take measures despite a pending procedure only under exceptional circumstances if it sees an urgent need for action to protect the rights and freedoms of data subjects.</p> |
|---|---|---|

| | | |
|--|--|--|
| <p><u>3. When referring the matter pursuant to paragraph 2, the supervisory authority may submit a draft measure to the lead authority.</u> Where the lead supervisory authority does not act on a draft measure referred to it pursuant to paragraph 1a, within a period of four weeks after having received the draft measure, the supervisory authority which has referred the matter, may submit the matter to European Data Protection Board under the consistency mechanism referred to in Article 57.</p> <p><u>4. Where, in the case referred to in paragraph 2, the concerned supervisory authority to which the complaint has been lodged considers the complaint as unfounded, it shall notify this to the lead supervisory authority. Where the lead supervisory authority objects to such finding, it may refer the case to the consistency mechanism within two weeks after having received the notification. Where a supervisory authority concerned has not objected within this period, it is deemed to be in agreement with the draft measure.</u></p> | <p><u>7. The participating supervisory authorities of the other Member States may comment on the draft compliance decision by the lead authority and/or object to it. Failure by a supervisory authority to respond within the six weeks' time limit set by the European Data Protection Board shall be deemed as a vote in favour of the draft (tacit agreement). The subsequent compliance decision by the lead authority shall be binding if all supervisory authorities of the Member States did not object. Objections shall set out the grounds for the decision to object. If one supervisory authority objects to the draft decision of the lead authority, any national supervisory authority, the European Commission or the European Data Protection Board may launch the cooperation procedure pursuant to Art. 58.</u></p> | <p>All national supervisory authorities should be consulted in the EDPB also during the non-compliance procedure. Individual national supervisory authorities should be bound by the lead authority's decision only if they expressly consent (in which case this decision becomes a decision of the consenting Supervisory authority and can be disputed before the national court), because corrective measures on national level are sufficient to redress a complaint of a data subject in this Member State. If the procedure does not lead to an EU-wide non-compliance decision, the European Commission, a national supervisory authority or the EDPB may initiate the cooperation procedure pursuant to Art. 58. The cooperation procedure is concluded by a non-binding EDPB opinion to be taken into account by all stakeholders.</p> |
|--|--|--|

| | | |
|---|---|--|
| <p><u>5. Where, in the case referred to in paragraph 2, the lead supervisory authority and the supervisory to which the complaint has been lodged, have reached agreement that the complaint is unfounded, the supervisory authority to which the complaint has been lodged, shall reject the complaint and notify the rejection to the complainant.</u></p> <p><u>6. In other cases, the supervisory authority to which a complaint has been lodged shall inform the data subject of the measure which the supervisory authority which is competent in accordance with Article 51(1) or acts as lead authority pursuant to paragraph 1 or 2 of Article 51a has adopted.</u></p> <p>Article 55 (Mutual assistance) – no changes</p> <p>Article 56 (Joint operations) – only minor redaction changes</p> | <p style="text-align: center;"><u>Article 56a</u></p> <p style="text-align: center;"><u>Judicial redress and remedies in the Union-wide compliance procedure</u></p> <p><u>1. The applicant of a Union-wide compliance procedure shall have the right to judicial remedies against the rejection by the lead authority pursuant to Article 56 (5) (b). Proceedings shall be brought before the courts of the Member State where the lead authority is established. The applicant shall have the right to judicial remedy against the decision of the European Data Protection Board brought before the General Court pursuant to Article 263 (4), Article 256 (1) TEU.¹</u></p> | <p>While the architecture of the German proposal is interesting there are several aspects that do not seem to be completely thought out.</p> <p style="text-align: center;"><u>b) The Presidency proposal:</u></p> <p>In a case where controller has establishments in several Member States or the processing is done in the context of one establishment but significantly affects data subject in other MS it firstly needs to be established which Supervisory Authorities is the lead authority (Article 51a). Where a complaint has been lodged to a supervisory authority which is not competent to deal with the matter the receiving supervisory authority needs to refer the matter to the lead supervisory authority, who shall prepare a decision (taking into account opinion of other supervisory authorities). The Supervisory authority to which the complaint has been lodged (if it agrees with the decision) has the obligation to notify the data subject of the decision which the lead authority adopted.</p> |
|---|---|--|

¹ This provision can be introduced as new Article after the provisions for the co-operation procedure at the EDPB.

| | | |
|--|---|--|
| <p style="text-align: center;">SECTION 2 CONSISTENCY Article 57 Consistency mechanism</p> <p>1. For the purpose set out in Article 46(1a), the supervisory authorities shall co-operate with each other through the consistency mechanism as set out in this section .</p> <p>1a. (...) <u>In a case referred to in paragraph 1 or 2 of Article 51a</u>, the <u>lead</u> supervisory authority (...) shall communicate a draft measure referred to in paragraph 1a of Article 54a to the European Data Protection Board and the Commission when <u>a supervisory authority concerned objects to a draft measure of the lead supervisory authority pursuant to paragraph 3 of Article 54a or paragraph 4 of Article 54b</u></p> <p>1b. (...).</p> | <p><u>2. Each data subject shall have the right to judicial remedy brought before the court of the Member State in which he /she is resident against its supervisory authority in case the supervisory authority refuses to take a measure due to a binding compliance decision. If the compliance decision was found in violation with the rules of this Regulation it shall not be binding for the supervisory authority of the Member State where the data subject has his/her residence. Each data subject shall have the right to judicial remedy against the decision of the European Data Protection Board brought before the General Court pursuant to Article 263 (4), Article 256 (1) TEU.</u></p> | <p>Where other supervisory authorities concerned object to the decision of the lead authority, the matter is referred to the EDPB who can issue a legally non-binding opinion. If the lead supervisory authority does not follow an opinion of the EDPB, Commission may issue implementing act of general scope for correct application of the Regulation.</p> |
|--|---|--|

| | | |
|--|--|---|
| <p>2. The supervisory authority competent for the supervision of the main establishment of the controller or processor which intends to adopt a measure aimed at producing effects in more than one Member State, shall communicate the draft measure to the European Data Protection Board and the Commission, when the measure:</p> <p>(a) (...);</p> <p>(b) (...);</p> <p>(c) aims at adopting a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 33(2b); or</p> <p>(ca) concerns a matter pursuant to Article 38(2b) whether a draft code of conduct or an amendment or extension to a code of conduct is in compliance with this Regulation; or</p> <p>(cb) aims to approve the criteria for accreditation of a body pursuant to paragraph 3 of Article 38a or a certification body pursuant to paragraph 3 of Article 39a;</p> <p>(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or</p> | <p><u>3. Member States, whose supervisory authorities objected to the decision of the European Data Protection Board have the right to judicial remedy brought before the Court of Justice pursuant to Article 263 (2) TEU.¹</u></p> <p><u>4. The applicant has the right to judicial redress against judgements which suspend the obligation to comply with a compliance decision.</u></p> <p style="text-align: center;"><u>Article 57</u></p> <p style="text-align: center;"><u>Union-wide Non-compliance Procedure</u></p> <p><u>1. Each supervisory authority may initiate the Union-wide non-compliance procedure to obtain a legally binding decision by the supervisory authorities of all Member States if in its opinion a certain data processing activity does not comply with this Regulation. Each supervisory authority shall initiate the Union-wide non-compliance procedure to obtain a legally binding decision if the said processing activities are related to the offering of goods or services to data subjects in several Member States and may substantially affect the free movement of personal data within the Union or the right of individuals to protection with regard to the processing of personal data.;</u></p> | <p>- The shortcomings of the Presidency’s proposal:</p> <p>One of the shortcomings of the nature of the Supervisory Authorities “notification” of the measures the “lead authority has adopted to the Data Subject is unclear. Can the decision of the lead authority be subject to judicial review in the Member State where data subject file the complaint before the Supervisory Authority or can it only be disputed before the national courts of the lead authority? This would in practice mean that the Portuguese citizen may file a complaint before CNPD but in cases where CNPD would not also be a lead authority he would need to go to another member state for judicial review! The German proposal seems to have quite an interesting aspect in providing that the decision of the lead authority is binding also binding for the supervisory Authorities involved in the EDPB procedure if they have not objected it. Hence the decision of the lead authority is also a national legal act of the Supervisory Authorities which were involved in the consistency procedure and can therefore also be disputed in front of the national courts in all of the Supervisory authorities which are bound by the decision of the lead authority.</p> |
|--|--|---|

¹ This provision can be introduced as new Article after the provisions for the co-operation procedure at the EDPB.

| | | |
|--|--|--|
| <p>(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or</p> <p>(f) aims to approve binding corporate rules within the meaning of Article 43.</p> <p>3. Where the competent supervisory authority does not submit a draft measure referred to in paragraphs 1a and 2 to the Board or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56, any supervisory authority concerned, the European Data Protection Board or the Commission may request that such matter shall be communicated to the European Data Protection Board .</p> <p>4. (...)</p> <p>5. Supervisory authorities and the Commission shall electronically communicate to the European Data Protection Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft measure, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.</p> | <p><u>2. To initiate Union-wide non-compliance procedure, the supervisory authority of a Member State shall issue a non-compliance decision. Such a decision may be</u></p> <p><u>(a) the result of an examination based on a data subject's complaint pursuant to Article 73 (5),</u></p> <p><u>(b) the result of an ex-officio examination by that supervisory authority, or</u></p> <p><u>(c) the negative result of a Union-wide compliance procedure conducted by the lead authority pursuant to Article 56 (2) at the request of a processor or controller according to Article 34 a (rejection pursuant to Article 56 (7) (b)).</u></p> <p><u>3. The competent supervisory authority shall forward the non-compliance decision to the European Data Protection Board and shall request the Board to ask the supervisory authorities of the other Member States to agree. The authority initiating the procedure shall thereby become the requesting supervisory authority.</u></p> | <p>- There may also be practical difficulties for the lead authority when it comes to preparing and adopting the intended draft measure in cases which concern or take place on a territory of another (non)lead authority. In such cases the lead authority will need to rely on the mutual assistance mechanism and eventually (if the decision of a lead authority can also be disputed before the national court of the non-lead supervisory authority) it will be difficult to defend this decision (which was prepared and adopted by the lead authority) before the national court, since the investigation, the draft of the decision was prepared by a lead authority. While Article 1a seems to guarantee proximity to the data subject on one hand and controller on the other, it seems to be lacking it when it comes to Supervisory Authorities.</p> |
|--|--|--|

| | | |
|--|---|--|
| <p>6. The chair of the European Data Protection Board shall without undue delay electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the European Data Protection Board shall, where necessary, provide translations of relevant information.</p> <p style="text-align: center;">Article 58</p> <p>Opinion by the European Data Protection Board</p> <p>1. (...)</p> <p>2. (...)</p> <p>3. (...)</p> <p>4. (...)</p> <p>5. (...)</p> <p>6. (...)</p> <p>6a. (...)</p> | <p><u>4. In its request to conduct a Union-wide non-compliance procedure, the requesting supervisory authority must describe and explain</u></p> <p><u>(a) the category of data processing in question,</u></p> <p><u>(b) the reasons for the opinion that the data processing in question violates the law,</u></p> <p><u>(c) the objective interest in a Union-wide decision, notably the importance of the data processing for a substantial number of data subjects concerned in more than one Member State or the existence of establishments in more than one Member State.</u></p> <p><u>5. The requesting supervisory authority has to inform the controller or processor about the intention to initiate a Union-wide non-compliance procedure one month before the procedure starts. The information shall contain recommendations how to ensure the protection of personal data and to demonstrate compliance with this Regulation. The right of the controller to initiate a Union-wide compliance procedure with the lead authority pursuant to Article 56 remains unaffected. If a Union-wide compliance procedure is initiated the non-compliance procedure is suspended. In exceptional circumstances, where there is an urgent need to act in order to protect rights and freedoms of data subjects, the supervisory authority may immediately adopt provisional measures in accordance with Article 53 for the territory of its own member state, as long as the compliance procedure is going on.</u></p> | |
|--|---|--|

| | | |
|---|---|--|
| <p>7. In the cases referred to in paragraphs 1a and 2 of Article 57, the European Data Protection Board shall issue an opinion on the subject- matter submitted to it in provided it has not already issued an opinion on the same matter. This opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. Regarding the draft measure circulated to the members of the Board in accordance with paragraph 6 of Article 57, a member which has not objected within the period indicated by the Chair, shall be deemed to be in agreement with the draft measure.</p> <p>7a. Within the period referred to in paragraph 7 the supervisory authority competent for the supervision of the main establishment shall not adopt its draft measure.</p> <p>7b. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1a and 2 of Article 57 and the Commission of the opinion and make it public.</p> | <p><u>6. The European Data Protection Board shall forward the authority's request to conduct a Union-wide non-compliance procedure to the other Member States' supervisory authorities without delay. The supervisory authorities shall decide within six weeks whether they agree with the requesting authority.</u></p> <p><u>7. If a participating supervisory authority agrees within the time limit pursuant to paragraph 6, the non-compliance decision by the lead authority shall be binding in the territory of that supervisory authority (explicit agreement).</u></p> | |
|---|---|--|

| | | |
|---|---|--|
| <p>8. The supervisory authority referred to in paragraphs 1a and 2 of Article 57 shall take utmost account of the opinion of the European Data Protection Board and shall within two weeks after receiving the opinion, electronically communicate to the chair of the European Data Protection Board whether it maintains or will amend its draft measure and, if any, the amended draft measure, using a standardised format.</p> <p>9. Where the supervisory authority concerned does not intend to follow the opinion, it shall inform the chair of the European Data Protection Board and the Commission within the period referred to in paragraph 8 and shall explain its refusal to follow the opinion.</p> <p>10. (...)</p> <p>11. (...).</p> | <p><u>8. The European Data Protection Board shall identify the result of the Union-wide non-compliance procedure after the deadline for submitting an agreement has passed. The Board shall inform the requesting supervisory authority, the supervisory authorities and the European Commission of the result of the Union-wide non-compliance procedure. The Board shall forward to the controller or processor in question all of the participating supervisory authorities' agreements and comments. The requesting supervisory authority shall inform the controller or processor of the result of the Union-wide non-compliance procedure.</u></p> <p><u>9. In order to bring about a uniform, Union-wide opinion, the requesting supervisory authority, the European Commission or the European Data Protection Board may within one month initiate the co-operation procedure pursuant to Article 58.</u></p> | |
|---|---|--|

| | | |
|--|--|--|
| <p style="text-align: center;">Article 59</p> <p style="text-align: center;">Opinion by the Commission</p> <p>(...)</p> <p style="text-align: center;">Article 60</p> <p style="text-align: center;">Suspension of a draft measure</p> <p>(...)</p> <p style="text-align: center;">Article 61</p> <p style="text-align: center;">Urgency procedure</p> <p>1. In exceptional circumstances, where the competent supervisory authority considers that there is an urgent need to act in order to protect rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Article 57 or the procedure referred to in Article 54a, immediately adopt provisional measures <u>intended to produce legal effects</u> (...) for the territory of its own Member State, with a specified period of validity. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them, to the European Data Protection Board and to the Commission.</p> | <p style="text-align: center;"><u>Article 57a</u></p> <p style="text-align: center;"><u><i>Judicial redress in the Union-wide non-compliance procedure</i></u></p> <p style="text-align: center;"><u><i>The controller or processor shall have the right to judicial remedies against non compliance decision pursuant to Article 57 (2). Proceedings shall be brought before the courts of the Member State where the requesting supervisory authority, which has initiated the non-compliance procedure, is established. The controller's or processor's possibility to seek legal redress shall remain unaffected by the launch of the co-operation procedure pursuant to Article 58.</i></u></p> | |
|--|--|--|

| | | |
|---|---|--|
| <p>2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion.</p> <p>3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.</p> <p>4. By derogation from paragraph 7a of Article 58, an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.</p> | <p style="text-align: center;"><u>Article 58</u></p> <p style="text-align: center;"><u>Co-operation Procedure</u></p> <p><u>1. Each supervisory authority, the European Commission and the European Data Protection Board may initiate the co-operation procedure in the following cases:</u></p> <p><u>(a) if the Union-wide compliance procedure (Article 56) did not lead to a Union-wide binding decision,</u></p> <p><u>(b) if the Union-wide non-compliance procedure (Article 57) did not lead to a Union-wide binding decision,</u></p> <p><u>(c) on adopting a list of the processing operations that are subject to the requirement for a data protection impact assessment pursuant to Article 33(2b)¹,</u></p> <p><u>(d) on approving the criteria for accreditation of a body pursuant to paragraph 3 of Article 38a or a certification body pursuant to paragraph 3 of Article 39a², or</u></p> | |
|---|---|--|

¹ Provisions regulating the procedure and legal consequences for this case have to be discussed.

² Provisions regulating the procedure and legal consequences for this case have to be discussed.

| | | |
|---|---|--|
| <p style="text-align: center;">Article 62</p> <p style="text-align: center;">Implementing acts</p> <p>1. The Commission may adopt implementing acts of general scope for:</p> <p>(a) <u>(...) the correct application of the Regulation concerning a matter referred to in point (a) of Article 57(1a), in relation to which the lead supervisory authority did not follow an opinion of the European Data Protection Board;</u></p> <p>(b) (...);</p> <p>(c) (...);</p> <p>(d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 57(5) and (6) and in Article 58(8). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p> <p>2. (...).</p> <p>3. (...).</p> | <p><u>2. If the Union-wide compliance procedure did not lead to a Union-wide binding decision pursuant to Article 56 (8) a decision shall be taken by the European Data Protection Board:</u></p> <p><u>(a) If less than one third of the supervisory authorities objected to the draft decision of the lead authority, the European Data Protection Board shall without delay issue the applicant the compliance decision. The compliance decision of the European Data Protection Board is binding for all supervisory authorities. The binding effect of the decision is limited by the results of a judicial review.</u></p> <p><u>(b) If one third or more of the supervisory authorities objected to the draft decision of the lead authority, the European Data Protection Board may submit a new draft which takes due account of the comments and objections. If the revised draft is also rejected by one third or more of the supervisory authorities, the European Data Protection Board shall communicate the results to the applicant. 3. If the Union-wide non-compliance procedure (Article 57) did not lead to a Union-wide binding decision, the European Data Protection Board shall issue a non-binding opinion pursuant to Article 58a.</u></p> | |
|---|---|--|

| Article 63 | Article 58a | |
|---|---|--|
| <p style="text-align: center;">Notification of measures adopted by the competent supervisory authority</p> <p>1. Without prejudice to paragraph 5 of Article 54b, the supervisory authority competent(...) or acting as lead supervisory authority for deciding on measures intended to produce legally binding effects shall notify such measure (...) that were adopted under the cooperation or consistency mechanism or the consultation mechanism referred to in Article 54a to the controller or processor concerned.</p> <p>1b. (...)</p> <p>1. (...).</p> <p>2. (...).</p> | <p style="text-align: center;">Opinion by the European Data Protection Board</p> <p>1. (...)</p> <p>2. (...)</p> <p>3. (...)</p> <p>4. (...)</p> <p>5. (...)</p> <p>6. (...)</p> <p>6a. (...)</p> <p><u>7. In the cases referred to in paragraph 3 of Article 58, the European Data Protection Board shall issue an opinion on the subject-matter submitted to it provided it has not already issued an opinion on the same matter. This opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board.</u></p> <p>7a. Within the period referred to in paragraph 7 the supervisory authorities shall not adopt any measures.</p> <p>7b. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authorities and the Commission of the opinion and make it public.</p> | |

| | | |
|--|---|--|
| | <p>8. The supervisory authorities shall take utmost account of the opinion of the European Data Protection Board and shall within two weeks after receiving the opinion, electronically communicate to the chair of the European Data Protection Board whether they intend to follow the opinion.</p> <p>9. Where a supervisory authority does not intend to follow the opinion, it shall inform the chair of the European Data Protection Board and the Commission within the period referred to in paragraph 8 and shall explain its refusal to follow the opinion.</p> <p>10. (...)</p> <p>11. (...).</p> <p style="text-align: center;"><i>Article 59</i></p> <p style="text-align: center;"><i>Opinion by the Commission</i></p> <p>(...)</p> <p style="text-align: center;"><i>Article 60</i></p> <p style="text-align: center;"><i>Suspension of a draft measure</i></p> <p>(...)</p> <p style="text-align: center;"><i>Article 61</i></p> <p style="text-align: center;"><i>Urgency procedure</i></p> <p style="text-align: center;"><i>[No changes to the text in Doc. 17831/13]</i></p> | |
|--|---|--|

| | | |
|--|--|---|
| | <p style="text-align: center;"><i>Article 62</i> Implementing acts <i>[No changes to the text in Doc. 17831/13]</i></p> | |
| | <p style="text-align: center;">SECTION 3 EUROPEAN DATA PROTECTION BOARD</p> | |
| | <p style="text-align: center;"><i>Article 64</i> European Data Protection Board</p> <p>1. A European Data Protection Board is hereby set up. <u>It shall have legal personality.</u></p> <p style="text-align: center;"><i>[No changes to paragraph 2 till 4] Article 65</i> Independence</p> <p style="text-align: center;">to</p> <p style="text-align: center;">Article 72 (Confidentiality)</p> <p><i>[No changes to the text of Article 64 to Article 72 in Doc. 17831/13]</i></p> | <p>DE Proposal – article 64:</p> <p>The question of legal personality is of importance when it comes to the question of effective legal address against the measures taken by EDPS. If the EDPB lacks legal personality appeals against its decisions would not be possible. With EDPB having legal personality judicial remedy against its decision can be brought before the General Court pursuant to Article 263(4) and 256(1) TEU since a decision by EDPB is a decision by a European institution.</p> |

| <p style="text-align: center;">CHAPTER VIII</p> <p style="text-align: center;">REMEDIES, LIABILITY AND SANCTIONS</p> | <p style="text-align: center;">CHAPTER VIII</p> <p style="text-align: center;">REMEDIES, LIABILITY AND SANCTIONS</p> | |
|--|--|--|
| <p style="text-align: center;"><i>Article 73</i></p> <p style="text-align: center;"><i>Right to lodge a complaint with a supervisory authority</i></p> <p>1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory <u>authority if the data subject considers that the processing</u> of personal data relating to him or her does not comply with this Regulation.</p> <p>1a. (...)</p> <p>2. (...)</p> <p>3. (...)</p> <p>4. Without prejudice to its duties under paragraph (b) of Article 52(1) and to Article 54b, when the supervisory authority to which a complaint has been lodged is not competent for a <u>measure intended to produce legal effects as referred to in paragraph 1a of Article 54a</u>, it shall refer the complaint to the supervisory authority which is competent under Article 51 or acts as <u>lead supervisory authority pursuant to paragraph 1 or 2 of Article 51a</u>.</p> | <p style="text-align: center;"><i>Article 73</i></p> <p style="text-align: center;"><i>Right to lodge a complaint with a supervisory authority</i></p> <p>1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority <u>in the Member State in which he or she is resident</u>, if the data subject considers that the processing of personal data relating to <u>him or her</u> does not comply with this Regulation.</p> <p>2. By way of exception to paragraph, for operations processed by a Member State's public authorities only the supervisory authority established in that Member State shall be competent.</p> <p>3. <u>The supervisory authority to which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint. Where the supervisory authority competent finds the complaint unfounded, it shall notify the complainant thereof and inform him of the reasons for the rejection and of the possibility of an judicial remedy pursuant Article 74. In all other cases the supervisory authority to which the complaint has been lodged may initiate a non-compliance procedure according to Article 57 (3).</u></p> | |

| | | |
|---|--|--|
| <p>5. The supervisory authority to which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint. Where the supervisory authority competent in accordance with Article 51 or paragraph 5 of Article 54b finds the complaint unfounded, the supervisory authority to which the complaint has been lodged shall notify the complainant thereof and inform him of the reasons for the rejection and of the possibility of an judicial remedy pursuant Article 74.</p> <p style="text-align: center;"><i>Article 74</i></p> <p style="text-align: center;"><i>Right to a judicial remedy against a supervisory authority</i></p> <p>1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a decision of a supervisory authority concerning them, including when the complaint has been rejected, in part or wholly.</p> | <p style="text-align: center;"><i>Article 74</i></p> <p style="text-align: center;"><i>Right to a judicial remedy against a supervisory authority</i></p> <p>1. <u>Without prejudice to any other administrative or non-judicial remedy, each</u> natural or legal person shall have the right to <u>an effective</u> judicial remedy against a decision of a supervisory authority concerning them in the country in which they are resident, including when the complaint has been rejected, in part or wholly; in case of operations processed by a <i>Member State's public authorities, in that State.</i></p> | |
|---|--|--|

| | | |
|---|---|--|
| <p>2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a judicial remedy where the supervisory authority competent in accordance with Article 51 does not deal with a complaint or does not inform the data subject within three months or any shorter period provided under Union or Member State law on the progress or outcome of the complaint lodged under Article 73.</p> <p>3. Proceedings against a decision of a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.</p> <p>4. (...)</p> <p>5. (...)</p> | <p>2. <u>Without prejudice to any other administrative or non-judicial remedy, each</u> data subject shall have the right to a judicial remedy, <u><i>in the country in which they are resident, obliging the supervisory authority</i></u> , where the supervisory authority does not <u>deal with a complaint or does not</u> inform the data subject within three months <u>or any shorter period provided under Union or Member State law</u> on the progress or outcome of the complaint <u>lodged under Article 73.</u></p> <p><u><i>3. If the processing of personal data was subject to a compliance decision pursuant to Art. 56 each data subject shall have the right to a judicial remedy pursuant to Article 74 Abs.1 aimed at a review of this decision as far as the rights of the data subject are concerned.</i></u></p> <p><u><i>4. Each controller or processor shall have the right to a judicial remedy against a decision of one or more supervisory authorities that adversely affects their interests. Where the decision has been taken pursuant to Article 56 Article 56a applies. Where the decision has been taken pursuant to Article 57 Article 57a applies.</i></u></p> <p><u><i>5. The Member States shall enforce final decisions by the courts referred to in this Article.</i></u></p> | |
|---|---|--|

Article 75

Right to a judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority under Article 73, a data subject shall have the right to an effective judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment (...). Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller is a public authority acting in the exercise of its public powers.
3. (...)
4. (...)

Article 76

Representation of data subjects

1. The data subject shall have the right to mandate a body, organisation or association, which has been properly constituted according to the law of a Member State and whose statutory objectives include the protection of data subjects' rights and freedoms with regard to the protection of their personal data, to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf.

1a. [Independently of a data subject's mandate or complaint, any body, organisation or association referred to in paragraph 1 shall have the right to lodge a complaint with the supervisory authority competent in accordance with Article 51 if it has reasons to consider that a personal data breach referred to in Article 32(1) has occurred and Article 32(3) does not apply.]

- 2. (...)
- 3. (...)
- 4. (...)
- 5. (...)

ROMANIA

RO welcomes the effort of the DE delegation to speed up the negotiations on the one stop shop mechanism. The German proposal is interesting and we appreciate that it brings positive elements which ensure advantages for the controllers (this matter being the main role of the one stop shop mechanism), but also proximity for the citizens.

Because of the new perspective rendered by the German proposal, the ideas expressed below represent some preliminary ideas that we outlined, following which, during the future technical working groups (DAPIX), we will express a position regarding the new proposal.

Referring to the proximity for the citizens, this represents an essential element for any future legislative act which will regulate the protection of personal data at European level. The proximity to the persons whose rights are guaranteed, ensures in itself an efficient protection of their private lives and, correspondingly, the absence of it would question the added value of such a legislative act (in comparison with the level of protection guaranteed by the Directive 95/46/EC).

The DE proposal offers positive elements concerning the procedure of cooperation among data protection authorities. We have some questions in what concerns the decision adopted by the EDPB during the procedure established at art. 58. According to this procedure, the decision EDPB should be applicable in all the member states, even though up to 1/3 of the member states oppose to the decision draft (point 2, letter a).

Regarding the possibility for the supervising authorities opposing to the decision draft to contest it before the court, it would be useful to clarify whether the expression: “The binding effect of the decision is limited by the results of a judicial review” from art. 58, point 2, (a), indeed ensures this possibility.

Moreover, regarding art 58, par 2, point (b), in what concerns the procedure to issue a new decision draft, which includes the observations expressed by at least 1/3 of the supervisory authorities, we propose to analyze the possibility that in case this new decision draft is still objected **by less** than 1/3 of the supervisory authorities, this shall be covered by the provisions of art. 58, point 2, (a) and only otherwise the EDPB shall communicate the results to the applicant. By doing that, similar situations would be dealt with in the same way.

SLOVAK REPUBLIC

One-stop-shop mechanism

SK and some other delegations repeatedly presented constitutional problem with the current layout of OSS mechanism. This problem also arises in the Slovak legislation and conflicts with the principle of sovereignty which does not allow for the decision of a foreign state to be applicable on the territory of the Slovak Republic. This is not a problem of primary application of the legislation of the European Union but a problem of awarding the power to a foreign state body to apply its decisions on the territory of another sovereign state. According to the Art. 14 of the Constitution of the Slovak Republic obligations may be imposed:

- a) by or pursuant to an Act, within its limits while preserving fundamental rights and freedoms,
- b) by an international treaty under Art. 7(4) which directly imposes rights and obligations to the natural persons or legal persons, or,
- c) by a Government regulation pursuant to Art. 120(2).

Abovementioned clearly states that the Constitution of the Slovak Republic does not allow the application of a decision of a foreign state which imposes obligations on its territory or to its citizens and therefore current layout of a one-stop-shop mechanism which proposes application of such decisions is unacceptable for us. We do not agree with the opinion of COM that the legislation of the European Union has priority over the national legislation in this case.

However after latest discussion where KOM and Presidency stated that the decision of lead DPA shall be binding only towards the controller of the main establishment and who shall be responsible for following of this decision by all of other establishments of the controller we are forced to reevaluate our opinion. Situation where the decision shall not be applied on the territory and towards the citizen of SK would be acceptable for us.

Nevertheless our opinion is that the aforementioned is not represented in the current text of the Regulation and therefore it is not possible to clearly deduce such application of the OSS mechanism. It is crucial for the text of the proposal to state such application in a clear and comprehensible manner which shall not cause apprehension and uncertainty of collision of the provisions of the Regulation and Constitutions of Member States.

Therefore we propose following amendment of Art. 51:

1aa. Measures of each Member State's supervisory authority referred to in paragraph 1 of Art. 51 shall be binding for the controllers or processor with main establishment on the territory where the supervisory authority is competent for the supervision exclusively.

We would like to join those delegations which expressed a need to elaborate provision on deciding of the lead DPA. We fully support the proposal of UK where such decision would be based on the same principle as it is in Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules (WP 108) in point 3.3.

Additional comments

The position of SK towards the one-stop-shop has been presented several times during last meetings of the working group and has not changed. Similarly as DK we also think that the reservations of both delegations were not solved and still persist. SK comments on current text of the presidency are in general consistent with our last comments.

Art. 53a

Similarly as several other delegations including SE, FR and IT, SK considers it appropriate to move content of this provision into recital. However we are not against such provision in the binding part of the Regulation, still we consider it redundant since all of the Member States have the question of formal aspect of decisions covered by their national legislation.

Art. 54b

Same as UK and PL our opinion is that parties to the amicable settlement should consist of DPA, controller/processor and data subject. In general however the text of the presidency in this area is heading towards the right direction.

Art. 62

SK would like to join NL, ES, IE, UK and HU in their opinion that it is necessary to clarify competencies of the EDPB and COM since current provisions are confusing and it is not sufficiently clear in what manner shall these competencies be applied in their mutual interaction.

Art. 73

In our opinion it is more rational and more suitable to award data subjects the right to submit a complaint only to competent DPA of one member state or to DPA of their habitual residence. However, at the same time we consider it necessary to ensure a possibility for data subjects to submit a complaint to DPA of a Member State which they have a relationship to from the point of view of their citizenship or mother tongue. Basically data subjects would be able to submit complaints to DPAs of three Member states at the most and not to all Member State which is a more rational solution for several obvious reasons.

German proposal

On the grounds of the extensiveness and complexity of changes proposed by German delegation we are forced to apply general scrutiny reservation. German proposal however has a potential to contribute to a solution to several key areas. Despite its potential similarly as some delegations we have significant doubts towards administrative and time burden of the proposed mechanism.

EDPB

Our opinion towards the EDPB is consistent with the opinion of the European Parliament which considers it necessary to lay down strong EPB with legal capacity for adopting legally binding decisions. Strong position of the EDPB is pivotal in ensuring the coordination of the one-stop-shop mechanism and only with EDPB with legal capacity to adopt binding measures it shall be possible to achieve purpose of this mechanism with the prevention of unnecessary administrative and time constrictions of the whole process. However in our opinion adoption of binding measures should be limited only to exceptional and complicated cases and in most cases the EDPB should be limited to coordination of the one-stop-shop mechanism

FINLAND

GENERAL REMARKS

FI welcomes the opportunity to submit written comments on one-stop-shop.

- The role of European Data Protection Board and the possibility of EDPB to function as an agency/body should be further examined. This in particular with a view of granting EDPB the possibility to issue binding decisions.
- While FI sees that main establishment authority can issue sanctions and warnings to main establishment controller, investigation powers should clearly remain in the competence of the local authority.
- While FI can support the underlying idea of the definition of the “main establishment” in Presidency’s proposal, FI sees that some inconveniences might follow when applying this model in practice. In other words, even if FI can support the aim of the Presidency proposal, FI would favour more practical approach in this question and would therefore prefer DE proposal for the definition of the main establishment authority. This would seem to lead to a more clear and precise outcome.

MORE DETAILED COMMENTS ON PRESIDENCY’S PROPOSAL

- It should be specified in article text that lead authority can issue the sanctions etc. only to the controller of the main establishment.

Competence for acting as lead supervisory authority

1. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State, the supervisory authority for the main establishment shall act as lead supervisory authority and shall be competent to decide on measures applying the powers conferred on it in accordance with the cooperation procedure foreseen in Articles 54a and 54b.

2. Where the processing of personal data takes place in the context of the activities of one establishment of a controller or processor in the Union and the processing substantially affects or is likely to affect substantially data subjects in more than one Member State, the supervisory authority of that establishment shall act as lead authority and shall be competent to decide on measures applying the powers conferred on it in accordance with Articles 54a and 54b.

3. Paragraph 1 shall not apply where the subject matter concerns only processing carried out in a single Member State other than the MS where the main establishment is located and involving only data subjects in that single Member State.

COMMENT: How would this paragraph apply to a situation where main establishment is located in the member state which is referred to in paragraph 3. See drafting proposal:

4. This article shall not apply where the processing is carried out by public authorities and bodies of a Member State. The only supervisory authority competent to exercise the powers conferred on it in accordance with this Regulation regarding a Member State's public authorities and bodies shall be the supervisory authority of that Member State.

Article 53(a):

General remarks

To find a compromise solution as regards this Article, FI supports those delegations who have suggested that the content of paras 2 and 3 of this Article would be removed to recitals. FI also sees that the applied articles could be added in the list in para 3. And instead of simply saying “indicate the supervisory authority” in point 3(b) it should be specified which supervisory authority.

Article 53a

Exercise of powers by the supervisory authority

- 1. The exercise of the powers conferred on the supervisory authority pursuant to Article 53 shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law.**

- 2. When exercising the powers referred to in Article 53, each supervisory authority shall act impartially, fairly and within a reasonable time. In particular each measure shall:**
 - (a) be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case and legitimate interests of the persons concerned;**
 - (b) respect the right of every person to be heard, before any individual measure which would affect him or her adversely is taken;**
 - (c) avoid superfluous costs and excessive inconveniences for the persons concerned;**
 - (d) be taken without undue delay.**

3. Each legally binding measure of the supervisory authority exercising the powers referred to in Article 53 shall be in writing and:

- (a) be clear and unambiguous;**
- (b) indicate the supervisory authority, which has issued the measure;**
- (c) indicate the time of issuance of the measure;**
- (d) bear the signature of the head or a member of the supervisory authority of a person authorised by him or her;**
- (e) give the reasons for the measure;**
- (ee) refer to the applied articles**
- (f) refer to the right of an effective remedy and give contact details of the competent court, indicating the form and time limits for such remedy.**

ARTICLE 54(a)

General remarks

FI finds it of utmost importance that it is clear which authority is competent to act and for example prepare a draft measure. As regards Article 54(a), only measure referred to in paragraph 1(a) would be the one a supervisory authority concerned is considering. Later in paras 2(b) and 2(ca) lead authority first submits the draft measure and adopts and notifies the draft measure referred to in para 1(a). It should be clarified that lead authority draws the draft measure and later on adopts the draft measure it has prepared. In case this has not been the intention but rather to give the possibility for the local authority to submit a draft measure to the lead authority, FI cannot agree with para 2(ca).

Furthermore, FI suggest that words “is being” would be inserted in para 1. See the drafting proposal. (Compare Art. 51(a)(2))

Cooperation between the lead supervisory authority and other supervisory authorities concerned

1. **In the cases referred to in paragraphs 1 and 2 of Article 51a, (...) the lead supervisory authority(...) shall cooperate with the supervisory authorities concerned by the processing in question in accordance with this article and with Article 54b in an endeavour to reach consensus(...). A supervisory authority is concerned by the processing, where there is an establishment of the controller or processor in its Member State or where a data subject residing in this Member State *is being or is likely to be substantially affected by the processing.*1a. Where, in a case referred to in paragraph 1 or 2 of Article 51a, *a supervisory authority concerned considers a measure intended to produce legal effects by applying the powers referred to in paragraphs 1, 1b and 1c of Article 53 as appropriate in view of the processing in question, it shall refer the matter to the lead supervisory authority.***

2. (...) **The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the supervisory authorities concerned and shall, without prejudice to Article 54b:**

- a) (...);
 - b) submit the *draft of a measure referred to in paragraph 1a* to all supervisory authorities (...)concerned **for their opinion;**
 - c) take utmost account of the views of the supervisory authorities (...);
- (ca) adopt and notify the measure referred to in paragraph 1a to the controller or processor.**

2a. The lead supervisory authority may request/ask at any time other concerned supervisory authorities to provide mutual assistance pursuant to Article 55, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. Where any of the supervisory authorities **concerned** objects, within a period of four weeks after having been consulted under paragraphs 1 or 2, to the draft measure **referred to in point (b) of paragraph 2**, this authority **shall** submit the matter to the consistency mechanism referred to in Article 57. Where a supervisory authority concerned has not objected within this period, it is deemed to be in agreement with the draft measure.

4. (...)

4a. (...)

4b. Where a concerned supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 61 shall apply.

5. The supervisory authority of the main establishment of the controller or processor and the other supervisory authorities concerned shall supply the information required un

MORE DETAILED COMMENTS ON DE PROPOSAL

- Non-compliance procedure could be further developed and the role of the EDPB as a part of it.
- FI suggests that both compliance and non-compliance -procedure would lead to a binding decision.
- In Article 74(2) formulation “obliging the supervisory authority” could be reconsidered.

Recital 96b

The lead authority should be competent to decide on measures applying the powers conferred on it in accordance with the provisions of this Regulation. In its capacity as lead authority, the supervisory authority should cooperate with the supervisory authorities concerned. The decision by the lead authority should be directed towards the main establishment as defined in this Regulation.

Article 51

Competence

1. Each supervisory authority shall be competent on the territory of its own Member State to perform the duties and to exercise the powers conferred on it in accordance with this Regulation, ~~without prejudice to Article 51a¹~~.
2. (...)
3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

¹ If the decision by the “lead authority” is to be directed towards the “main establishment” the wording in paragraph 1 “without prejudice to Article 51a” is misleading. The wording would suggest that in some cases a supervisory authority of another Member State would be competent to perform duties and exercise powers on the territory of the Member State mentioned in the article.

Article 51a

Competence for acting as the lead supervisory authority

1. Without prejudice to Article 51, where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State **(or if the processing substantially affects or is likely to affect substantially data subjects in more than one Member State)**¹, the supervisory authority of the main establishment of that processing shall act as lead supervisory authority.
2. **The lead supervisory authority shall with regards to processing referred to in paragraph 1, be competent to decide on measures applying the powers conferred on it in accordance with Article 53. A decision by the lead supervisory authority shall be directed towards the main establishment responsible for the processing referred to in paragraph 1.**²
3. The lead supervisory authority shall comply with the cooperation procedure foreseen in Articles 54a and 54b.
4. This article shall not apply where the subject matter concerns only processing carried out in a single Member State and involving only data subjects in that Member State, or where the processing is carried out by public authorities and bodies of a Member State.³

¹ Wording moved from paragraph 2 of doc. 5882/14 REV3.

² New paragraph in order to clarify the competence of the lead supervisory authority as well as the scope of the decision meaning that a decision of the lead authority concerns the processing subject to the main establishment's control. The main establishment is then responsible for complying with the decision of the lead authority, which does not have extra territorial competence.

³ Processing not covered by the One stop shop – gathered in one paragraph (par. 3 and 4 of doc. 5882/14 REV3).