



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 22 November 2013**

**16626/13**

---

---

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

---

---

**LIMITE**

**DATAPROTECT 177  
JAI 1042  
MI 1063  
DRS 208  
DAPIX 145  
FREMP 192  
COMIX 625  
CODEC 2675**

**NOTE**

---

from:	Presidency
to:	JHA Counsellors/COREPER
No. prev. doc.:	15604/13 DATAPROTECT 157 JAI 964 MI 951 DRS 192 DAPIX 135 FREMP 170 COMIX 579 CODEC 2440 15802/13 DATAPROTECT 159 JAI 975 MI 971DRS 194 DAPIX 137 FREMP 174 COMIX 586 CODEC 2469
No. Cion prop.:	5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7 COMIX 61 CODEC 219
Subject:	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - The one-stop-shop mechanism: partial general approach on essential concepts

---

**Background**

1. The one-stop-shop principle, as laid down in Section II of Chapter VI, has been discussed by the Working Party on Information Exchange and Data Protection (DAPIX) at meetings of 8-9 January, 27 March, 3-4 July, 9-10 September, 17-18 October, 7-8 and 20 November 2013. Various delegations have produced documents on this and the compilation of comments on Chapters VI and VII is set out in 7105/5/13 REV 5 DATAPROTECT 28 JAI 182 MI 170 DRS 42 DAPIX 49 FREMP 24 COMIX 141 CODEC 476. The annex contains the relevant articles of Chapters VI, VII and VIII; those for which the Presidency has proposed new changes, are in **underlined bold text**. Where text has been deleted, this is indicated by (...). Where existing text has been moved, this text is indicated in italics. The text is subject to a general scrutiny reservation by: CZ, DE, DK, FR, FI, HU, LU, MT, NO, PT, RO, SE, SI, SK and UK.

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

- a) in important transnational cases the draft Regulation should establish a one-stop shop mechanism in order to arrive at a single supervisory decision, which would be fast, ensure consistent application, provide legal certainty and reduce administrative burden.
- b) further expert work on this should continue along a model in which a single supervisory decision is taken by the 'main establishment' supervisory authority but the exclusive jurisdiction of that authority would be limited to the exercise of certain powers;
- c) the Working Party should explore methods for enhancing the 'proximity' between individuals and the decision-making supervisory authority by involving the 'local' supervisory authorities in the decision-making process. This proximity is an important aspect of the protection of individual rights;

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

3. The one-stop-shop principle purports to be an advantage for businesses: it aims at ensuring compliance with the Regulation and legal certainty for enterprises. The Presidency suggests a simple and clear mechanism to be constructed on the basis of the building blocks set out hereafter.

#### **Extension of competence of 'local' supervisory authority to processing substantially affecting data subjects on its territory**

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

5. Under the current legal regime, the 1995 Data Protection Directive gives no competence to the Member State where a person lodges a complaint regarding an alleged data breach, if there is no establishment or equipment in that Member State. In the 1995 Directive this follows indirectly from the definition of territorial applicable law. Article 4(1) (a) of that Directive gives as the main criterion to trigger the applicability of national law the fact that 'the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State'.

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

- the establishment of the controller or processor;
- the fact that the data processing substantially affects data subjects on its territory; or
- the fact that a controller not established in the Union is processing personal data.

7. The proximity of which the importance was emphasised at the October JHA Council meeting is ensured by the second criterion. This criterion will ensure that a supervisory authority is competent whenever 'its' data subjects are substantially affected by the processing of their personal data by a controller or processor, even if it is established in another Member State. Obviously such competence should exist only regarding processing by a controller/processor in another Member State that extends to data subjects in other Member States and should not allow supervisory authorities to 'rule' on processing that took place in the context of the use of services or purchase of goods in another Member State

### **Powers of the supervisory authority**

8. Regarding the processing activities of a controller or processor that fall within the scope of the one-stop-shop mechanism, the debate has so far concentrated on which powers should the supervisory authority of the main establishment exercise exclusively, that is excluding the exercise of those powers by local authorities. In the course of previous discussions on the Commission proposal for a one stop-shop principle, one of the criticisms which has been voiced on this principle related to a perceived transfer of powers and the related need to enforce decisions of another Member State. In view of the discussions held and in view of the analysis of the possible exclusive exercise of different types of power by the main establishment supervisory authority, the Presidency thinks that the one-stop-shop mechanism can be constructed along the elements set out hereafter.

9. *monitoring powers*: to be exercised by each supervisory authority regarding processing on for which it is competent, that is processing by establishment of the controller or processor on its territory or substantially affecting data subjects on its territory.
10. *investigatory powers*: in accordance with the territoriality principle set out at the beginning of Article 51, these can be exercised by each supervisory authority only on their own territory. In case a main establishment authority needs to have investigations carried out on the territory of another Member state, it will have to request this to the supervisory authority of that Member State via mutual assistance channels.
11. *authorisation powers*: under the current draft of the Regulation, the authorisation procedure for Binding Corporate Rules (BCRs - Article 43) and contractual clauses (Article 42(2)(c) and (d)) provides that they need to be submitted by the main establishment supervisory authority to the EDPB. This is not the case for prior consultation (Article 34) which, following authorisation, can be used by the controller. In the future, the Working Party may look into ways of expanding authorisation powers so as to enable controllers to apply for a confirmation of compliance with the legal requirements of the Regulation.
12. The substantive articles on authorisation will be redrafted so as to distinguish between a one-Member State authorisation and an EU-wide authorisation. The one-stop-shop mechanism will apply only to EU-wide authorisations, for which only the main establishment supervisory authority would be competent. In cases of an EU-wide authorisation or confirmation of compliance, all 28 supervisory authorities will be involved through the European Data Protection Board (EDPB). In this case the controller should directly apply to the supervisory authority of the main establishment, which should forward the application to the EDPB. All supervisory authorities receive the application and a draft measure prepared by the main establishment authority.
13. *corrective powers*: to be exercised by each supervisory authority regarding processing on for which it is competent, that is processing by an establishment of the controller or processor on its territory or substantially affecting data subjects on its territory. The inclusion of the latter criterion will on the one hand allow the data subject to have its complaint dealt with by its 'local' supervisory authority and on the other hand enable the supervisory authority dealing with the complaint to act 'on the spot'.

14. Whilst this solution ensures proximity for the exercise of corrective powers, it may not allow to adequately address the underlying problem in all situations. First, a purely local approach will be insufficient in case the local authority dealing with a complaint is not the one competent for the (main) establishment deciding on the impugned processing<sup>1</sup>. Were it is the 'local' supervisory authority to impose sanctions in such case, it would be imposing them on an establishment which is not responsible for the decision leading to the faulty processing. A second type of case where a purely local approach will not be satisfactory is where there is no establishment on the territory of the Member State of the 'local' supervisory authority, as that authority will not have the power to carry out any investigations regarding the controller or processor and neither to power to enforce any sanctions. While it may adopt corrective measures, it will not have the possibility to serve these (not even warnings and/or reprimands) on the controller/processor, as it is not be 'present' within the territory of that Member State.

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

15. The main establishment supervisory authority should therefore have the exclusive power to adopt corrective measures where the main establishment was decision-making authority, but in all other cases the 'local' supervisory authority should be able to adopt corrective powers. In order to ensure the proximity to data subject also in the case where the main establishment supervisory authority has the exclusive competence to adopt corrective measures, all concerned supervisory authorities should be involved in deciding on the draft corrective measure and the 'local' supervisory authority have the right to trigger the consultation mechanism by submitting draft corrective measure to the main establishment supervisory authority. Before adopting a corrective measure, the main establishment authority will endeavour to reach consensus with the other concerned authorities. To this end, the main establishment authority shall share all relevant information with the concerned authorities and submit to them the draft measure and take utmost account of their views. Moreover, the local authority should still have the power to adopt corrective measures in case the supervisory authority of the main establishment of the controller or processor does not act within six weeks after the matter has been referred to the to European Data Protection Board.

---

<sup>1</sup> A second type of situation could be distinguished, namely where the physical processing takes place in another Member State. However, this will only be a problem where the supervisory authority dealing with complaint will not be competent regarding the main establishment, as the main establishment should have the power to control the processing taking place in another Member State.

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

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

#### **Decision-making process via EDPB**

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

#### **Judicial redress and judicial review**

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

20. Regarding *judicial review* proximity is ensured through the competence of any supervisory authority to act upon a complaint from a data subject resident on its territory and substantially affected by data processing. All supervisory authorities will be competent to hear a complaint and act upon it, not only if there is an establishment on the territory of that Member State, but also when data processing substantially affects data subjects on its territory. It will therefore be sufficient to state in Article 73(1) of the draft Regulation that data subjects would have the right to lodge a complaint with the competent supervisory authority. Judicial review under Article 74 is closely linked to the power of the supervisory authority of that Member State and should therefore be possible only in the courts of the Member State of the supervisory authority concerned.

21. Regarding *judicial redress*, it has been established that the general rules on jurisdiction (in particular those flowing from Brussels I) provide sufficient grounds of jurisdiction for the courts of the Member state to order measures against the controller or processor responsible for the alleged data protection violation. The articulation of the provisions on jurisdiction in this Regulation with the Brussels I Regulation is clarified in recital 118a

If the court of habitual residence of the data subject has no jurisdiction over the controller or processor responsible for the alleged data protection violation, the exercise of a judicial remedy against or the seeking of compensation from a controller or processor will result in a judgment that needs to be enforced in the territory of the Member State where the controller or processor has an establishment. This is also possible under the Brussels I Regulation.

22. *Delegations are invited to confirm their approval for the one-stop-shop mechanism on the basis of the elements outlined above.*

---

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)**

(Text with EEA relevance)

- 93) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should co-operate with each other and the Commission.

**93a) Regarding processing by a controller or processor established in the Union, each supervisory authority should be competent on the territory of its own Member regarding processing that takes place in the context of the activities of an establishment of that controller or processor on its territory. It should also be competent regarding processing substantially affecting data subjects on its territory, notably when the processing is targeted at a significant number of data subjects in the territory of that Member State, who may use the goods or services offered by that controller or processor in their own Member State. It should not be competent regarding processing which affected data subjects staying on its territory when the use of the service or purchase of goods to which the processing is related, took place in another Member State.**



94) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for adopting decisions further to authorisation and corrective powers as regards the controller or processor, in order to increase the consistent application, provide legal certainty and reduce the administrative burden for such controllers and processors. This should not apply in relation to controllers that are not established in the Union; their representative may be addressed by each supervisory authority, in addition to or instead of the controller.

The competence of the single supervisory authority should include measures intended to produce legal effects such as the authorisation of binding corporate rule and of transfers of personal data to third countries or international organisations, administrative fines and other sanctions. However, the competence of that supervisory authority should not encompass the competence for the enforcement of its decisions, on the territory of another Member State, unless in the context of joint operations and allowed by the Member State concerned.

95) The competent authority for the supervision of the processing and the related decisions, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment. However, the supervision of the processing by a public authority or body should be carried out solely by the supervisory authority or the supervisory authorities of the Member State where the public authority or body is established.

96) While this Regulation applies also to the activities of national courts, the competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks (...), in accordance with national law.

97) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. Member States may determine other duties related to the protection of personal data under this Regulation. Investigative powers of supervisory authorities (...) should be exercised in conformity with Union law and national law. This concerns in particular the requirement to obtain a prior judicial authorisation.

98) Each supervisory authority should deal with complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.

Where the supervisory authority to which the complaint has been lodged is not the competent supervisory authority, the competent supervisory authority should closely co-operate with the supervisory authority to which the complaint has been lodged according to the provisions on co-operation and consistency laid down in this Regulation. In such cases, the competent supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority to which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

99) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as data subjects.

- 100) The supervisory authorities should assist each other in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market.
- 101) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The requested supervisory authority should be obliged to respond to the request in a defined time period.
- 102) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to exercise its **corrective** powers as regards processing operations which substantially affect a significant number of data subjects in several Member States (...). It should also apply where any supervisory authority concerned or the Commission requests that such matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.
- 103) In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a (...) majority of its members so decides or if so requested by any supervisory authority concerned or the Commission.
- 104) (...)
- 105) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.

- 106) The application of this mechanism should be a condition for the (...) enforcement of the (...) decision by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, mutual assistance and joint operations might be carried out between the supervisory authorities *concerned* on a bilateral or multilateral basis without triggering the consistency mechanism.
- 107) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities without voting rights. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.
- 111) Every data subject should have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, and have the right to an effective judicial remedy in accordance with Article 47 of the Charter of Fundamental Rights if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint or does not act where such action is necessary to protect the rights of the data subject. The supervisory authority to which the complaint has been lodged shall deal with the complaint, to the extent appropriate, for example by clarifying the queries of the data subject. In case the supervisory authority to which the complaint has been lodged is not competent for the supervision of the controller or processor, it shall transmit the complaint without undue delay to the competent supervisory authority in another Member State.<sup>2</sup>

---

<sup>2</sup> NL said that recital 111 was an important recital and that it depended on the context which DPA that should be competent, e.g. for labour law the SA of the habitual residence would be the most appropriate DPA.

- 112) Where a data subject considers that his or rights under this Regulation are infringed, he or she should have the right to mandate a body, organisation or association which aims to protect the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State, to lodge a complaint on his or her behalf with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects. Such a body, organisation or association should have the right to lodge, independently of a data subject's complaint, a complaint where 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.
- 113) Each natural or legal person should have the right to an effective judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and shall be conducted in accordance with the national law of that Member State . Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.
- 114) (...)
- 115) (...)
- 116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority acting in the exercise of its public powers.
- 117) (...).

- 118) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where he establishes fault on the part of the data subject or in case of force majeure. The concept of damage should be broadly interpreted in the light of the case law of the Court of Justice of the European Union in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law<sup>3</sup>.
- 118a) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, **general jurisdiction rules such as those of Regulation No 1215/2012** should not prejudice the application of such specific rules.

---

<sup>3</sup> Further to DE suggestion. COM scrutiny reservation.

*Article 4*  
*Definitions*

(13) ‘main establishment’ means

- as regards the controller, the place of its central administration in the Union, unless the decisions on the purposes (...) and means of the processing of personal data are taken in an other establishment of the controller in the Union. In this case the latter shall be considered as the main establishment. If no decisions as to the purposes (...) and means of the processing of personal data are taken in the Union, (...) the place where the main processing activities in the context of the activities of an establishment of the controller in the Union take place<sup>4</sup>;
- as regards the processor, the place of its central administration in the Union and, if the processor has no central administration in the Union, the place where the main processing activities in the context of the activities of an establishment of the processor take place;
- Where the controller exercises also activities as a processor, the supervisory authority of the main establishment of the controller shall be considered as the main establishment for the supervision of processing activities;
- Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking shall be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking;

---

<sup>4</sup> BE, CZ DE, EE and SK scrutiny reservation: they expressed concerns about this definition, which might be difficult to apply in practice. Regarding the first indent, BE and FR, AT and SE preferred the previous version. IE remarked this place may have no link with the place where the data are processed. DE also remarked that in the latter scenario, the Commission proposal did not determine which Member States' DPA would be competent. CZ thought the definition should be deleted.

## SECTION 2

### COMPETENCE<sup>5</sup>, DUTIES AND POWERS

#### *Article 51* *Competence<sup>6 7</sup>*

1. Each supervisory authority shall, on the territory of its own Member State, be competent to perform the duties and exercise the powers conferred on it in accordance with this Regulation regarding:
  - a) processing (...) in the context of the activities of an establishment of the controller or processor on the territory of its own Member State;
  - b) processing substantially affecting data subjects on its territory<sup>8</sup>; or
  - c) as regards processing by a controller not established in the European Union, any processing referred to in paragraph 2 of Article 3 which is related to data subjects on its territory.

---

<sup>5</sup> GR thought it would be better to refer to jurisdiction rather than competence.

<sup>6</sup> Scrutiny reservation by DE, DK, EE, ES, FR, HU, NL, PT and UK. Some delegations (BG, CY, DE, GR, NL and LU) supported the principle of the main-establishment rule (aka as the one-stop-shop principle), but had many questions of understanding as to its practical implementation. Other delegations (BE, CZ, ES, FR, IT, AT, PT, RO and SI) had a more critical attitude and entered a reservation. One of the main questions was whether the allocation of competence to the DPA of the main establishment was exclusive and whether it also implied a rule of applicable law (DE, ES). A practical question was that of the language regime which would govern the co-operation between the DPAs and the communication with the controllers and the data protection. All delegations seemed to agree that at any rate the establishment of such a rule could not lead to the exercise of investigative powers by the DPA of one authority in the territory of another Member State.

<sup>7</sup> At the request of several delegations, COM indicated that the main-establishment rule under this paragraph would not apply to controllers established outside the EU. In the view of the Commission, this constituted an incentive for non-EU controllers to establish themselves in the EU in order to avail themselves of the benefit of the main establishment rule.

<sup>8</sup> See recital 93a. Several delegations feared that this criterion would lead to a multiplication of competence: DK, EE, IE, .LU, NL, RO and UK. COM reservation as this wording would have the effect of limiting the competence of DPAs and would be contrary to the Charter of Fundamental Rights.



- 1a. 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 processing concerned was decided by the main establishment**, the supervisory authority competent for the supervision of the main establishment of that controller or processor shall be exclusively competent for the adoption of corrective measures pursuant to paragraph 1b of Article 53. Where a supervisory authority other than that of the main establishment of the controller or processor **finds that the processing concerned was decided by the main establishment and is of the opinion that measures pursuant to paragraph 1b of Article 53 need to be adopted regarding this processing**, it shall refer the matter to the supervisory authority competent for the supervision of the main establishment of the controller or processor. When referring the matter, that supervisory authority may submit a draft measure referred to in paragraph 1b of Article 53.
- 1b. 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, the supervisory authority competent for the supervision of the main establishment of that controller or processor shall be exclusively competent for adopting authorisations referred to in paragraph 1c of Article 53 that are intended to have an effect in other Member States.
- 1c. 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.
2. (...)<sup>9</sup>.
- 2a. (...)<sup>10</sup>.
- 2b. (...)<sup>11</sup>.

---

<sup>9</sup> Moved to Article 54a (5).

<sup>10</sup> Moved to Article 54b (2).

<sup>11</sup> Moved to Article 54a (7).

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity<sup>12</sup>.

Article 52

**Duties**<sup>13</sup>

1. Without prejudice to other duties set out under this Regulation<sup>14</sup>, each supervisory authority shall<sup>15</sup>:
- (a) monitor and enforce the application of this Regulation;
  - (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*;
  - (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*<sup>16</sup>
  - (ac) promote the awareness of controllers and processors of their obligations under this Regulation;
  - (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*;

---

<sup>12</sup> FR, HU, NL, RO and UK scrutiny reservation. DE suggested adding " other matters assigned to courts for independent performance. The same shall apply insofar as judicially independent processing has been ordered, approved or declared admissible", as the derogation must apply whenever courts' work falls within the scope of their institutional independence, which is not only the case in the core area of judicial activity but also in areas where courts are assigned tasks specifically for independent performance.

<sup>13</sup> DE, IT, AT, PT and SE scrutiny reservation. UK thinks the term 'functions' rather than 'duties' should be used.

<sup>14</sup> New text as paragraphs (f) to (i) have been deleted as these duties were already laid down elsewhere in the Regulation.

<sup>15</sup> The Presidency shall seek to draft a recital in order to clarify that Member States may allocate other tasks to DPAs. DE thought it preferable to use the words 'at least' in the chapeau. See also new point (g) in paragraph 1.

<sup>16</sup> Moved from Article 52(1)(j) as this a duty rather than a power from the DPA.

- (b) deal with complaints<sup>17</sup> lodged by a data subject, or body, organisation or association representing a data subject in accordance with Article 73<sup>18</sup>, 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<sup>19</sup>, in particular if further investigation or coordination with another supervisory authority is necessary;
- (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;
- (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;
- (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;
- (f) (...);
- (fa) (...);
- (g) (...);
- (ga) (...);
- (gb) (...);
- (gc) (...);
- (gd) (...);
- (h) (...);

---

<sup>17</sup> IT scrutiny reservation on the term complaint; UK thought the emphasis should be on complaint-resolution.

<sup>18</sup> BE suggested limiting this to the data subject itself.

<sup>19</sup> IT suggested fixing a 10-weeks period for dealing with the complaint.

- (ha) (...);
  - (hb) (...);
  - (i) (...);
  - (j) contribute to the activities of the European Data Protection Board;
  - (k) *issue opinions<sup>20</sup> as well as fulfill any other duties related to the protection of personal data.*
2. (...).
  3. (...).
  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.
  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.
  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<sup>21</sup>. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request<sup>22</sup>.

---

<sup>20</sup> Some delegations (IE, PL) thought this was worded too generally.

<sup>21</sup> EE pointed out that under its constitution this required an act of parliament. NL and RO also thought this should be left to Member States.

<sup>22</sup> DE, NL and SE reservation: this could be left to general rules.

*Article 53*  
**Powers**<sup>23 24</sup>

1. Each Member State shall provide by law that<sup>25</sup> its supervisory authority shall have at least<sup>26</sup> the following monitoring powers:
- (a) *to order the controller and the processor<sup>27</sup>, and, where applicable, the representative to provide any information it requires for the performance of its duties;*
  - (aa) *to carry out data protection audits<sup>28</sup>;*
  - (b) 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;
  - (c) (...)

---

<sup>23</sup> DE, NL, RO, PT and SE scrutiny reservation; SE thought this list was too broad. Some Member States were uncertain (CZ, DE, RO and UK) or opposed (DK, IE) to categorising the DPA powers according to their nature.

<sup>24</sup> Several Member States (DE, FR, SI) stated that it was unacceptable that the supervisory authority would be able to exercise these powers vis-à-vis public authorities. DE thought a distinction should be drawn between powers with regard to public and non-public bodies. Direct powers of instruction in respect of public bodies subject to supervisory and judicial control, which might therefore lead to conflicts, would be problematic for Germany. Moreover, consideration also needs to be given to the delimitation between this proposal and the proposal for a Directive on police and judicial affairs, which accords fewer powers to the supervisory authorities in some respects.

<sup>25</sup> Suggested amendment in order to allay the concern from Member States (FR, NL) that they should be able to specify in their national law, as has been the case under the 1995 Data Protection Directive, the exact scope of, conditions and guarantees for the exercise of these powers. COM reservation.

<sup>26</sup> Further to BG suggestion, supported by EE, IT, NL, to make this an indicative list. RO argued in favour of the inclusion of an explicit reference to the power of DPAs to issue administrative orders regarding the uniform application of certain data protection rules. COM and ES scrutiny reservation on 'at least' in paragraphs 1 and 1a.

<sup>27</sup> NL thought that all the powers listed in para. 1 should also be available vis-à-vis others than controllers and processors.

<sup>28</sup> CZ, IT, PL and SK scrutiny reservation. CZ and PL pleaded for a recital explaining that audit could be understood as inspection. NL indicated that such audits could also be carried out by an external office, but the Presidency points out that the current drafting does not preclude this.

- (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*<sup>29</sup>;
- 1a. Each Member State shall provide by law that its supervisory authority shall have at least<sup>30</sup> the following investigatory powers:
- (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;*
- (b) *to obtain access to any premises of the controller and the processor , including to any data processing equipment and means.*
- 1b. Each Member State shall provide by law that its supervisory authority shall have the following corrective powers:
- (a) *to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;*
- (b) *to issue reprimands*<sup>31</sup> *to a controller or processor where processing operations have infringed provisions of this Regulation;*<sup>32</sup>
- (c) (...);
- (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;*

<sup>29</sup> BE suggested adding the power to oblige the controller to communicate the personal data breach to the data subject.

<sup>31</sup> EE, IT, PL, SE and SK scrutiny reservation.

<sup>32</sup> PL scrutiny reservation on points (a) and (b).

- (e) to impose a temporary or definitive limitation on processing<sup>33</sup>;
- (f) to order the suspension of data flows to a recipient in a third country or to an international organisation<sup>34</sup>;
- (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.*
- 1c. Each Member State shall provide by law that its supervisory authority shall have the following authorisation powers:
- (a) authorise standard data protection clauses referred to in Article 34, or in point (c) of Article 42(2);
- (b) authorise contractual clauses referred to in Article 34, or in point (d) of Article 42(2);
- (c) approve binding corporate rules pursuant to Article 43.
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<sup>35</sup>.
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<sup>36</sup>, in order to enforce the provisions of this Regulation.

---

<sup>33</sup> NL scrutiny reservation. The Presidency suggests to use the word 'limitation' so as to accommodate concerns relating to the compatibility with the freedom of expression.

<sup>34</sup> SK reservation.

<sup>35</sup> The reference to national law will allow Member States to apply their procedural rules (cf. remarks by BE, DE, ES) and should also allay concerns regarding self-incrimination.

<sup>36</sup> DE, FR and RO reservation on proposed DPA power to engage in legal proceedings. UK scrutiny reservation. CZ reservation on the power to bring this to the attention of the judicial authorities.

4. (...) <sup>37</sup>

5. (...)

*Article 54*

*Activity report*

Each supervisory authority shall draw up an annual report<sup>38</sup> on its activities. The report shall be transmitted to the government<sup>39</sup> and the national parliament and shall be made available to the public, the Commission and the European Data Protection Board.

---

<sup>37</sup> DE thought paras 3 and 4 should be deleted.

<sup>38</sup> This article does not detract from the possibility for Member States to provide under national law that other, extraordinary reports may also be conveyed to the parliament and the government. However, the Presidency agrees with SI that there no need to oblige Member States to do so, certainly as there is a risk of an 'overkill' of reports.

<sup>39</sup> SE proposal; ES suggested adding 'other authorities designated under national law'.



**CHAPTER VII<sup>40</sup>**  
**CO-OPERATION AND CONSISTENCY**  
**SECTION 1**  
**CO-OPERATION**

**Article 54a**

**Cooperation between the main establishment authority and other supervisory authorities  
regarding the exercise of corrective powers<sup>41</sup>**

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, the supervisory authority of the main establishment of the controller or processor, to which a matter regarding the exercise of the corrective powers has been referred in accordance with paragraph 1a of Article 51, shall cooperate with the supervisory authorities of the Member States concerned in an endeavour to reach consensus on the cases set out hereafter.
2. When preparing and deciding on a measure referred to in paragraph 1b of Article 53, the authority **competent for the main establishment** shall:
  - a) share all relevant information with the supervisory authorities of the Member States concerned;
  - b) submit the draft measure to all supervisory authorities of the Member States concerned;
  - c) take utmost account of the views of the supervisory authorities of the Member States concerned.

---

<sup>40</sup> AT and FR scrutiny reservation on Chapter VII.

<sup>41</sup> BE, CY, DE, EE, FR, FI, RO, PT and NL scrutiny reservation.

3. Where any of the supervisory authorities has objected, within a period of **four** weeks after having been consulted under paragraphs **1** or **2**, to the draft measure, this authority may 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. 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.**
- 4a.** **If the supervisory authority of the main establishment of the controller or processor does not act within six weeks after the matter has been referred to the to European Data Protection Board, the supervisory authority which has referred the matter in accordance with paragraph 1a of Article 51, may adopt a measure referred to in paragraph 1b of Article 53. It shall take the utmost account of the opinion of the Board, in case the Board has issued an opinion on the matter.**
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.

Article 55

**Mutual assistance**<sup>42</sup>

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations. This shall apply in particular where the supervisory authority to which the complaint has been lodged is not the authority of the main establishment of the controller or processor. Mutual assistance shall also cover the provision of information on the conduct of investigations where the controller or processor has establishments in several Member States or where data subjects in several Member States are likely to be affected by processing operations by the controller or processor.<sup>43</sup>
2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without undue delay and no later than one month<sup>44</sup> after having received the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation (...).

---

<sup>42</sup> DE, NL SE and UK scrutiny reservation. Several other delegations indicated that further clarity was required on this fundamental Article and the concept of mutual assistance, and announced text proposals: EE pleaded for much more detailed rules on mutual assistance, as is already the case in civil and criminal law. AT, supported by DE, declared that it had no specific problem with this Article, but that, in general, there was a need to follow developments in relation to CoE Convention No. 108.

<sup>43</sup> ES requested that the added text be taken out.

<sup>44</sup> ES reiterated its suggestion to reduce it to 15 days. PT supported the suggestion of two weeks, with a possibility of adding more time, if needed. RO, on the other hand, found one month too short, and requested SE remarked that this timeline might be unrealistic in some cases. COM indicated that it was only a deadline for replying, but that paragraph 5 allowed longer periods for executing the assistance requested. UK requested a timetable, indicating deadlines.

3. The request for assistance shall contain all the necessary information<sup>45</sup>, including the purpose of the request and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.
4. <sup>46</sup>A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:
  - (a) it is not competent for the subject-matter of the request or for the measures it is requested to execute<sup>47</sup>; or
  - (b) compliance with the request would be incompatible with the provisions of this Regulation or with Union or Member State law to which the supervisory authority receiving the request is subject.
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to respond to the request. In cases of a refusal under paragraph 4, it shall explain its reasons for refusing the request<sup>48</sup>.
6. Supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means<sup>49</sup>, using a standardised format.
7. No fee shall be charged for any action taken following a request for mutual assistance. Supervisory authorities may agree with other supervisory authorities rules for indemnification by other supervisory authorities for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.<sup>50</sup>

---

<sup>45</sup> EE and SE scrutiny reservation.

<sup>46</sup> SE indicated further scrutiny was required as to whether other grounds of refusal were required. UK thought that this paragraph was drafted in much too absolute a fashion.

<sup>47</sup> Several delegations stressed the importance of establishing which is the competent DPA: DE, EE, SE, SI. NL and IT asked for further clarification.

<sup>48</sup> RO scrutiny reservation.

<sup>49</sup> PT (supported by RO) suggested adding "*or other means if for some reason, electronic means are not available, and the communication is urgent*"

<sup>50</sup> PT, UK and DE asked for clarification in relation to the resources needed / and estimate of costs.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 within one month of receiving the request<sup>51</sup> of another supervisory authority, the requesting supervisory authority may adopt a provisional measure<sup>52</sup> on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board and the Commission in accordance with the consistency mechanism referred to in Article 57<sup>53</sup>.
9. The supervisory authority shall specify the period of validity of such a provisional measure which shall not exceed three months<sup>54</sup>. The supervisory authority shall, without delay, communicate such a measure, together with its reasons for adopting it, to the European Data Protection Board and to the Commission in accordance with the consistency mechanism referred to in Article 57.
10. The Commission may specify the format and procedures for mutual assistance referred to in this article and 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 paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)<sup>55</sup>.

---

<sup>51</sup> RO found this deadline too short.

<sup>52</sup> LU requested more clarification with regard to what would happen if this provisional measure were not confirmed.

<sup>53</sup> EE, FR, RO, and UK reservation. DE scrutiny. UK did not find the drafting sufficiently clear, for instance regarding which authority would be competent and action on other Member States territory. COM specified that this Article would apply specifically in bilateral relations (whereas Article 56 would cover joint operations), the underlying philosophy being to avoid extraterritorial activity.

<sup>54</sup> DE asked for deletion of this deadline; the measure should be withdrawn if the conditions for imposing it were no longer fulfilled.

<sup>55</sup> DE, IT, EE, CZ and NL reservation. EE questioned whether implementing acts were necessary for this purpose. ES reminded about its proposal for an Article 55a.

*Article 56*  
***Joint operations of supervisory authorities***<sup>56</sup>

1. The supervisory authorities may, where appropriate, conduct joint operations, including joint investigations and joint enforcement measures in which members or staff from other Member States' supervisory authorities are involved.
  
2. In cases where the controller or processor has establishments in several Member States or where [a significant number of<sup>57</sup>] data subjects in **more than one** Member States are likely to be **substantially** affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint operations, as appropriate. The competent supervisory<sup>58</sup> authority shall invite the supervisory authority of each of those Member States to take part in the joint operations concerned and respond to the request of a supervisory authority to participate without delay.<sup>59</sup>

---

<sup>56</sup> IT requested a specification in this Article that this was also about multilateral cooperation. FR asked for a clearer distinction between Articles 55 and 56. DE, EE, PT and UK scrutiny reservation. Several delegations (DE, LV, NL, SE, IT, UK) supported the idea of joint operations, but thought more details needed to be clarified. DE and EE referred to a criminal law model of a joint investigation team. LU indicated it was not convinced of the added value of joint investigations. UK requested to make sure that these mechanisms would work in practice and drew the attention to the fact that paragraphs 1 and 3 were discretionary, whereas paragraph 2 was binding, and that this was confusing and potentially contradictory.

<sup>57</sup> COM reservation; more criteria should be added. IT, supported by PL, FR, BE and CZ suggested stressing the multilateral aspect by adding text.

<sup>58</sup> LU asked for a clarification of who would be the lead authority. UK stated that it seemed like a mix of Art. 51(1) and 51(2) competences.

<sup>59</sup> SE entered a favourable scrutiny reservation on this paragraph.

3. A supervisory authority may, in compliance with its own Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the seconding supervisory authority's law. Such investigative powers may be exercised only under the guidance and in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. (...)<sup>60, 61</sup>
- 3a. Where, in accordance with paragraph 1, staff of a supervisory authority are operating in another Member State, the Member State of the operating supervisory authority shall be liable for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.
- 3b. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the supervisory authority whose staff have caused damage to any person in the territory of another Member State shall reimburse the latter in full any sums it has paid to the victims or persons entitled on their behalf.
- 3c. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 3b, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement of damages it has sustained from another Member State<sup>62</sup>.
4. (...)

---

<sup>60</sup> SI and GR suggestion.

<sup>61</sup> DE, LU, PT and COM scrutiny reservation on the deletion of this last phrase.

<sup>62</sup> Inspired by Article 3 of the Council Framework Decision of 13 June 2002 on joint investigation teams. PL and UK reservation on paras. 3a, 3b and 3c.

- 5.<sup>63</sup> Where a joint operation is intended and a supervisory authority does not comply within one month with the obligation laid down in the second sentence of paragraph 2, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 51(1).
6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5, which shall not exceed three months. The supervisory authority shall, without delay, communicate such a measure, together with its reasons for adopting it, to the European Data Protection Board and to the Commission in accordance with the consistency mechanism referred to in Article 57.

## SECTION 2

### CONSISTENCY<sup>64</sup>

#### *Article 57*

#### *Consistency mechanism<sup>65</sup>*

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<sup>66</sup>.

---

<sup>63</sup> NL asked whether the measures of paragraphs 5 and 6 were really necessary. EE suggested a merger of the two paragraphs.

<sup>64</sup> BE, IT, SK and SI scrutiny reservation. BE reservation on the time required for a consistency mechanism procedure. DE parliamentary reservation and BE and UK reservation on the role of COM in the consistency mechanism.

<sup>65</sup> EE, FI, LU, NL and UK scrutiny reservation.

<sup>66</sup> CZ, DE, ES thought that supervisory authorities of third countries for which there is an adequacy decision should be involved in the consistency mechanism; if third countries participated in the consistency mechanism, they would be bound by uniform implementation and interpretation.



- 1a. 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, the supervisory authority competent for the supervision of the main establishment of that controller or processor, shall communicate a draft measure referred to in paragraph 1b of Article 53 to the European Data Protection Board and the Commission when data subjects in one or more other Member States have substantially been affected **or are likely to be substantially affected** by the processing for which it intends to adopt a measure pursuant to paragraph 1b of Article 53. **It shall not be obliged to do so if the matter has already been dealt with in the cooperation mechanism under Article 54a to the satisfaction of all supervisory authorities involved**<sup>67</sup>.
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:
- (a) (...);
  - (b) (...);
  - (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*
  - (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
  - (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;
  - (d) *aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or*

---

<sup>67</sup> New text aimed at addressing concerns voiced by FR, IT, PL and UK that this should be limited to cases where a coordination mechanism implemented by the lead authority does not result a solution acceptable to all supervisory authorities concerned.

- (e) *aims to authorise contractual clauses referred to in point (d) of Article 42(2);*  
*or*
- (f) *aims to approve binding corporate rules within the meaning of Article 43.*
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<sup>68</sup>, the European Data Protection Board or the Commission may request that such matter shall be communicated to the European Data Protection Board<sup>69</sup>.
4. (...)
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.
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.*

---

<sup>68</sup> BE, IT, SE, SI, SK and PL thought the scope of this paragraph should be limited so as to limit the number of cases.

<sup>69</sup> LU proposed restricting this to cases where the coordination mechanism implemented by the competent authority did not allow for a solution to be reached; ES referred to cases where the other authorities did not agree with the proposal of the competent(/lead) authority.

*Article 57a*

**Identification of the supervisory authority competent for the main establishment**

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 authority referred to in paragraphs 1a and 1b of Article 51. The authority shall communicate its reply to the other supervisory authorities concerned.
  
2. Where there are conflicting views between the supervisory authorities concerned on which supervisory authority is exclusively competent in accordance with paragraphs 1a and 1b of Article 51, any of the supervisory authorities concerned may communicate the matter to the European Data Protection Board. The European Data Protection Board shall issue an opinion on the identification of the supervisory authority of the main establishment in accordance with Article 58.

*Article 58*

***Opinion by the European Data Protection Board***<sup>70</sup>

1. (...)
2. (...)
3. (...)
4. (...)
5. (...)
6. (...)
- 6a. (...)

---

<sup>70</sup> NL and UK scrutiny reservation.

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<sup>71</sup>. This opinion shall be adopted within one month<sup>72</sup> 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.**
- 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.
- 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.
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 amends its draft measure and, if any, the amended draft measure, using a standardised format.
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.
10. (...)
11. (...).

---

<sup>71</sup> ES suggested deleting the possibility for one DPA requesting an opinion from the EDPB, but keeping this one-stop-shop possibility for the Commission.

<sup>72</sup> RO and GR proposed two months.

*Article 59*  
***Opinion by the Commission***<sup>73</sup>

(...)

*Article 60*  
***Suspension of a draft measure***<sup>74</sup>

(...)

*Article 61*  
***Urgency procedure***<sup>75</sup>

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 pursuant to points (a) and (b) of paragraph 1 of Article 53 and points (d), (e) and (f) of paragraph 1b of Article 53 for the territory of its own Member State<sup>76</sup>, 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<sup>77</sup>.

---

<sup>73</sup> Deleted in accordance with the request from BE, CZ, DE, ES, SE and UK. COM and FR reservation on deletion.

<sup>74</sup> Deleted at the suggestion of BE, CZ, DE, ES, IT, SE and UK. PT scrutiny reservation. COM and FR reservation on deletion.

<sup>75</sup> DE scrutiny reservation. COM explained that the urgency procedure was an essential part of the consistency mechanism. The existence of an urgency procedure was welcomed by several delegations (DE, ES, IT, NL), but also gave rise to many questions. There was lack of clarity surrounding the criteria which could warrant the taking of provisional measures (DE, FR, PT), in particular by another DPA. The need to respect certain procedural guarantees (e.g. giving notice to the data controller) prior to the taking of provisional measures was emphasised by FR.

<sup>76</sup> COM scrutiny reservation.

<sup>77</sup> The conditions under which the EDPB needed to be informed also gave rise to questions (GR, ES). COM stated the obligation only existed in cross-border one-stop-shop mechanism cases.

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.
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.
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.

#### *Article 62*

#### ***Implementing acts***

1. The Commission may adopt implementing acts of general scope for:
  - (a) (...)<sup>78</sup>.
  - (b) (...);
  - (c) (...);
  - (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).

2. (...)
3. (...)

---

<sup>78</sup> COM reservation on deletion.

Article 63

**Notification of measures adopted by the main establishment supervisory authority**<sup>79</sup>

- 1a. The supervisory authority competent for the supervision of the main establishment of that controller or processor shall notify the measures referred to in paragraphs 1a and 1b of Article 51 that were adopted under the **cooperation or consistency mechanism** to the controller or processor concerned.
- 1b. The supervisory authority to which a complaint has been lodged shall inform the data subject of the measure which the authority referred to in paragraph 1 has adopted.
1. (...).
2. (...).

---

<sup>79</sup> EE and SI reservation; DE and DK scrutiny reservation.

### SECTION 3

## EUROPEAN DATA PROTECTION BOARD<sup>80</sup>

#### *Article 64*

#### *European Data Protection Board<sup>81</sup>*

1. A European Data Protection Board is hereby set up.
2. The European Data Protection Board shall be composed of the head<sup>82</sup> of one supervisory authority of each Member State and of the European Data Protection Supervisor<sup>83</sup>.
3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative.
4. The Commission<sup>84</sup> shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative without voting rights. The chair of the European Data Protection Board shall, communicate the Commission the activities of the European Data Protection Board.

---

<sup>80</sup> Several Member States (BE, DE, IT, PL and PT) pleaded in favour of granting the EDPB the power to take legally binding decisions in the context of the consistency mechanism and do away with the proposed Commission power to intervene. It was argued that the DPAs should have the same independence vis-à-vis the Commission, as vis-à-vis the Member States' authorities. COM argued that it was legally impossible under the T(F)EU to confer such powers on the EDPB.

<sup>81</sup> The term 'Board' seems inappropriate and could be replaced by Committee.

<sup>82</sup> BE, supported by CZ, SE and SI, suggested adding "*or his/her representative*". IT suggested referring to Art. 68(2).

<sup>83</sup> NO pleaded in favour of the participation of the associated States. COM replied that the modalities for such participation were provided for in the association agreement.

<sup>84</sup> IT pleaded in favour of also including the Council and the Parliament.



*Article 65*

***Independence***

1. The European Data Protection Board shall act independently when performing its tasks pursuant to Articles 66 and 67.<sup>85</sup>
2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody<sup>86</sup>.

*Article 66*

***Tasks of the European Data Protection Board***

1. The European Data Protection Board shall promote the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular<sup>87</sup>:
  - (a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;
  - (b) examine, on its own initiative or on request of one of its members<sup>88</sup> or on request of the Commission<sup>89</sup>, any question covering the application of this Regulation and issue guidelines, recommendations and best practices<sup>90</sup> in order to encourage consistent application of this Regulation;

---

<sup>85</sup> UK and SI scrutiny reservation.

<sup>86</sup> DE scrutiny reservation.

<sup>87</sup> DE suggested adding the provision of an opinion on the level of data protection in third countries or international organisations. UK expressed concerns about the extensive list of tasks in a period of scarce resources. IT wanted it to figure that the list was not exhaustive.

<sup>88</sup> FR suggested that controllers be added here. However a controller can always ask 'its' DPA to submit a certain issue to the DPA.

<sup>89</sup> Some Member States (IT, DE) thought that, if Commission requests were included here, a similar possibility for the Council and the Parliament should be provided.

<sup>90</sup> FR expressed the opinion that it would be preferable to have a legally binding text.

- (ba) draw up guidelines for supervisory authorities concerning the application of measures referred to in point (c) of paragraph 1 of Article 53 and in paragraph 1b of Article 53 and the fixing of administrative fines pursuant to Articles 79 and 79a<sup>91</sup>;
- (c) review the practical application of the guidelines, recommendations and best practices referred to in points (b) and (ba);
- (ca) encourage<sup>92</sup> the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 38 and 39;<sup>93</sup>
- (cb) give the Commission an opinion on the level of protection in third countries or international organisations;<sup>94</sup>
- (d) issue opinions on draft measures of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;
- (e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;
- (f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;
- (g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide;

---

<sup>91</sup> RO, SE and UK scrutiny reservation. UK and SE inquired how this would be possible in relation to national law. CZ and SI noted that the method stated would not be appropriate in relations to individuals, and suggested adding "for undertakings".

<sup>92</sup> The term, that a couple of delegations found too weak, has been overtaken from Articles 38 and 39. IT, FR and UK entered a scrutiny reservation in view of the fact that these two Articles have not been finalised.

<sup>93</sup> RO a scrutiny reservation.

<sup>94</sup> This point was supported by a number of delegations. IT scrutiny reservation on paras. (cb) and (d).

2. Where the Commission requests advice from the European Data Protection Board, it may indicate a time limit, taking into account the urgency of the matter.
3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.
4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

#### *Article 67*

##### ***Reports***

1. (...).
2. The European Data Protection Board shall draw up an annual report regarding the protection of natural persons with regard to the processing of personal data in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, the Council and the Commission.
3. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).

#### *Article 68*

##### ***Procedure***

1. The European Data Protection Board shall take decisions<sup>95</sup> by a simple majority of its members (...).
2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements.

---

<sup>95</sup> Some delegations suggested replacing this term that could give rise to confusion, with another, such as for instance "resolution". COM would consider an alternative.

*Article 69*

***Chair***

1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members (...).<sup>96</sup>
2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable once.<sup>97</sup>

*Article 70*

***Tasks of the chair***

1. The chair shall have the following tasks<sup>98</sup>:
  - (a) to convene the meetings of the European Data Protection Board and prepare its agenda;
  - (b) to ensure the timely performance of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.
2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairpersons in its rules of procedure.

*Article 71*

***Secretariat***

1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat<sup>99</sup>.

---

<sup>96</sup> COM found this problematic and maintained its reservation on deletion.

<sup>97</sup> Further to BE proposal. NL thought that also the case where a chair or a deputy chairperson ceases to be a member of the European Data Protection Board[/Committee], should be addressed by the Regulation. However, this may be left to national law of the Member state concerned. COM and SK scrutiny reservation.

<sup>98</sup> BE suggesting adding another task, namely the chair's role towards the exterior.

<sup>99</sup> DE, EE, FR, ES, RO, PT, SI, SK and UK reservation on entrusting the EDPS with the EDPB secretariat. The risk of conflicts of interest of EDPS staff was also raised. FR and UK inquired about the costs. NL scrutiny reservation.

2. The secretariat shall provide analytical, administrative and logistical support to the European Data Protection Board under the direction of the chair.
3. The secretariat shall be responsible in particular for:
  - (a) the day-to-day business of the European Data Protection Board;
  - (b) the communication between the members of the European Data Protection Board, its chair, and the Commission and for communication with other institutions and the public;
  - (c) the use of electronic means for the internal and external communication;
  - (d) the translation of relevant information;
  - (e) the preparation and follow-up of the meetings of the European Data Protection Board;
  - (f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board.

*Article 72*

***Confidentiality***<sup>100</sup>

1. The discussions<sup>101</sup> of the European Data Protection Board shall be confidential.
2. Access to documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001.

---

<sup>100</sup> DE, EE, ES, RO, PL, PT, SE and UK reservation: it was thought that the EDPB should operate in a manner as transparent as possible and a general confidentiality duty was obviously not conducive to this. The Presidency thinks this article should be revisited once there is more clarity on the exact role and powers of the board, including the question whether the EDPS shall ensure the Secretariat.

<sup>101</sup> IT scrutiny reservation: it suggested replacing this term with 'minutes' or 'summary records', thereby distinguishing between confidentiality of decision-making and access to documents.

## CHAPTER VIII

### REMEDIES, LIABILITY AND SANCTIONS<sup>102</sup>

#### *Article 73*

#### ***Right to lodge a complaint with a supervisory authority<sup>103</sup>***

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 competent in accordance with Article 51<sup>104</sup>, if the data subject considers that the processing of personal data relating to him or her does not comply with this Regulation<sup>105</sup>.
- 1a. The supervisory authority to which a complaint has been lodged shall not take any measure [referred to in paragraph 1b of Article 53] if a possible violation of the same rights related to the same processing activities is already being examined by a court in accordance with Article 74, provided the data subject is party to these proceedings<sup>106</sup>.
2. (...)
3. (...)

---

<sup>102</sup> AT, FR, EE, ES and RO scrutiny reservation.

<sup>103</sup> BE, CY CZ, EE, IE, LY, PT and SI scrutiny reservation.

<sup>104</sup> The reference to article 51 allows to make a complaint to the DPA of the habitual residence, as that that DPA is competent whenever data subjects on its territory are affected by processing. BG, IE, PL and IT scrutiny reservation on this reference. BG, IT and LU though that the data subject should be able to lodge a complaint with any DPA without limitation since the protection of personal data was a fundamental right.

<sup>105</sup> DE, supported by NL, suggested adding "when its rights are not being respected".

<sup>106</sup> COM reservation. The Presidency is aware that an analogous rule for parallel proceedings will have to be established for the case where the same case is pending before another DPA. This is, however, intrinsically linked to the one-stop-shop mechanism. AT feared this paragraph 1a could lead to forum-shopping. SI thought this could be set out in a recital.

4. Whithout prejudice to its duties under paragraph 1 (b) of Article 52<sup>107</sup>, when the supervisory authority to which a complaint has been lodged is not competent for the supervision of the controller or the processor, it shall ex officio transmit the complaint to the supervisory authority which is competent under Article 51<sup>108</sup>.
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 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<sup>109</sup>.

#### *Article 74*

#### ***Right to a judicial remedy against a supervisory authority<sup>110</sup>***

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<sup>111</sup>.

---

<sup>107</sup> This reference is intended to address concerns raised by BG, CZ, HU that the DPA should not be a mere post box but it should decide when to forward the complaint or when to undertake measures. DK thought that the non-competent DPA could verify the complaint and see if there were some misunderstandings.

<sup>108</sup> ES, FR and IT reservation. Recital 111 clarifies that DPA to which the complaint was lodged and that is not the competent authority should not be a pure letter box but should at least take a preliminary look at the complaint.

<sup>109</sup> NL and FR scrutiny reservation. Article 54c (2) already provides for a general duty for the supervisory authority with which a complaint has been lodged to notify the data subject of any measures taken (i.e. the scenario of a 'positive' reply by the DPA).

<sup>110</sup> ES, PT and SI reservation. EE, IT and UK scrutiny reservation.

<sup>111</sup> DE, supported by SE, suggested adding: 'by which it is adversely affected'.

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<sup>112</sup> 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<sup>113</sup> on the progress or outcome of the complaint lodged under Article 73.<sup>114</sup>
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<sup>115116</sup>.
4. (...)
5. (...)<sup>117</sup>

#### *Article 75*

#### ***Right to a judicial remedy against a controller or processor***<sup>118</sup>

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<sup>119</sup> 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.

---

<sup>112</sup> COM reservation.

<sup>113</sup> SI indicated that under its law the DPA was obliged to reply within two months.

<sup>114</sup> SE scrutiny reservation. BE reservation. BE said that there was a link to Article 53 and the main establishment and the DPA of the habitual residence. Support from NL. IT thought that paragraphs 1 and 2 overlapped. NO wanted to delete paragraph 2 since a court review would endanger the independency of the DPA.

<sup>115</sup> IT suggests stating that proceedings may be brought before the courts of the Member state where the natural or legal person has his/her habitual residence or is established.

<sup>116</sup> In view of the reservations from BE, ES and FR, the reference to national law has been kept only in recital 113

<sup>117</sup> COM reservation on deletion of paragraphs 4 and 5. DE scrutiny reservation on deletion of paragraphs 4 and 5.

<sup>118</sup> DE, EE, PL, PT, SI and SK scrutiny reservation. ES, IT reservation.

<sup>119</sup> ES asked how judicial remedy would be interpreted and how a missed deadline or that there will be no judicial review would be considered.



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 (...) <sup>120</sup>. 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. <sup>121</sup>
3. (...)
4. (...)

*Article 76* <sup>122</sup>

**Representation of 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, <sup>123</sup> to lodge the complaint on his or her behalf <sup>124</sup> and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf <sup>125</sup>].

---

<sup>120</sup> In view of the concerns raised, the reference to national law has been kept only in recital 113

<sup>121</sup> ES wanted to know how the last sentence would apply in practice. With reference to habitual residence in Article 75, and the possibility for the data subject to lodge a complaint in any MS, the UK wanted to know it that meant that the data subject could seek judicial remedy in any Member State.

<sup>122</sup> DE, ES, PT and SI scrutiny reservation. CZ, EE, IT, NL, SI and UK thought this article was superfluous.

<sup>123</sup> COM said that consumer organisations and data protection organisations enhance fundamental rights so it was important that they could lodge complaints.

<sup>124</sup> IT scrutiny reservation.

<sup>125</sup> DE parliamentary reservation; BE, EE reservation and IT scrutiny reservation. EE, supported by SE, thought that the data subject could choose anybody to represent her/him so this drafting was a limitation so a reference to national law was needed. Support from SE.

- 1a. [Independently of a data subject's mandate or complaint, any body, organisation or association referred to in paragraph 1<sup>126</sup> shall have the right to lodge a complaint with the supervisory authority competent in accordance with Article 51<sup>127</sup> 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.<sup>128</sup>].
2. (...)
3. (...)
4. (...)
5. (...)<sup>129</sup>

### Article 76a

#### Suspension of proceedings<sup>130</sup>

1. Where a competent court of a Member State has reasonable grounds to believe that proceedings concerning the same processing activities are being conducted in another Member State, it shall<sup>131</sup> contact the competent court in the other Member State to confirm the existence of such proceedings.

---

<sup>126</sup> PL asked how an organisation could know about a breach. PT did not want to exclude the possibility of an organisation to lodge complaint if that was provided in national law but meant that the wording was not clear.

<sup>127</sup> COM reservation on limitation to competent supervisory authority.

<sup>128</sup> This paragraph was moved from Article 73(3). BE, EE, FR reservation. BG, DE, IT, LU, NL, PT and UK scrutiny reservation. UK in particular queried whether such possibility would also be open to an association when the data subject itself considered that the reply he/she had received was satisfactory. ES on the contrary thought that this possibility should not be limited to data breaches. UK meant that paragraph 1 was sufficient. For SE it was not acceptable that an organisation etc. had an independent right to lodge a complaint.

<sup>129</sup> COM scrutiny reservation on deletion of paragraphs 3 to 5. FR reservation on the deletion of paragraphs 3 to 4.

<sup>130</sup> AT, BE, EE, ES, FI, FR, IT, NL, PT and SE scrutiny reservation. ES thought that *lis pendens* necessitated the same persons, same proceeding, same object of dispute and same claim and that that could be difficult to establish. UK, supported by FR, cautioned against having a too prescriptive text, support from FR SE thought that GDPR should not regulate *lis pendens*, instead it should be up to the DPA and MS courts to decide. For LU this was a question of judicial cooperation between judicial authorities. NO and FR asked how this text related to Regulation No 44/2001 and the Lugano Convention FI considered that it was necessary to have rules on this question in GDPR.

<sup>131</sup> LU suggested to replace "shall" with "may".

2. Where a possible violation of the same rights related to the same processing activities is already being examined by a court in another Member State, the competent court may suspend<sup>132</sup> its proceedings concerning a natural and/or legal person provided these persons are also party to the proceedings in the other Member State.

*Article 77*

***Right to compensation and liability<sup>133</sup>***

1. Any person who has suffered <sup>134</sup> damage <sup>135</sup> as a result of a processing operation which is non compliant<sup>136</sup> with this Regulation shall have the right to receive compensation from the controller or processor<sup>137</sup> for the damage suffered.<sup>138</sup>

---

<sup>132</sup> NL and PL thought that it was difficult to force courts to stay proceedings waiting for another court to decide. NL asked how it was possible for a court to know that another case was going on elsewhere. COM thought that limitation to "same parties" was not appropriate here.

<sup>133</sup> Several Member States (DE, NL and UK) have queried whether there was an EU concept of damage and compensation or whether this was left to Member State law. IT suggested specifying that these rules are to be applied according to national law, support from CZ, NL, RO and SI. COM thinks that it has to be left to ECJ to interpret these rules and concepts. FR scrutiny reservation; FR questioned the division of responsibilities and the link to Articles 24 and 25 and national law in this field as well as the principle of subsidiarity.

<sup>134</sup> DE and SK suggested adding "material or immaterial/moral". NO suggested clarifying this in a recital.

<sup>135</sup> BE asked whether a violation of the principles of the Regulation was enough to constitute a damage or whether the data subject had to prove a specific damage (obligation de moyens ou de résultat). COM said that the data subject had to prove the damage.

<sup>136</sup> COM reservation as the current draft (contrary to the initial version and the 195 Directive) no longer embodies the principle of strict liability.

<sup>137</sup> DE suggested restricting the possibility to seek compensation from the processor to cases where, in violation of point (a) of paragraph 2 of Article 26, the processor has processed personal data contrary to or in the absence of instructions from the controller. ES suggested adding a reference to 'a right to exercise a direction action', but the Presidency thinks this I already encompassed in the current draft.

<sup>138</sup> SE considered that Article 77 was unclear and wanted to know whether both an economic and immaterial damage was covered.

2. <sup>139</sup>Where more than one controller or processor or a controller and processor are involved in the processing which gives rise to the damage, each controller or processor shall be jointly<sup>140</sup> and severally liable for the entire amount of the damage This is without prejudice to recourse claims between controllers and/or processors<sup>141</sup>.
3. The controller or the processor may<sup>142</sup> be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage<sup>143</sup>.

---

---

<sup>139</sup> IE queried why the reference to Article 24(2) had been removed and then the second sentence had been added: what the purpose to bring a claim against all of them and then sort out the individual responsibility?

<sup>140</sup> UK thought that one controller or processor might be more responsible than another so it should be allowed for a relative responsibility. SE said that according Directive 95/46 (Article 23) the burden of proof and division of responsibility between the controller and the processor it was only the controller that was held responsible.

<sup>141</sup> SI reservation: SI thought this paragraph could be deleted and left entirely to national law.

<sup>142</sup> PL thought this should be turned into a mandatory provision.

<sup>143</sup> DE and PL thought this paragraph needed to be further elaborated. DE in particular thought that the relationship to Article 39 needed to be further clarified. SI thought an arrangement for strict liability in the case of processing by public bodies should be inserted into this paragraph.