Council of the European Union

Brussels, 13 November 2014
(OR. en)

Interinstitutional File:
2012/0011 (COD)

14788/1/14
REV 1

LIMITE

DATAPROTECT 154
JAI 816
MI 816
DRS 141
DAPIX 156
FREMP 187
COMIX 579
CODEC 2113

NOTE

From:	Presidency
To:	Working Party on Information Exchange and Data Protection
No. prev. doc.:	10139/14 DATAPROTECT 79 JAI 357 MI 450 DRS 71 DAPIX 68 FREMP 101 COMIX 276 CODEC 1346
No. Cion doc.:	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

I. Introduction

1. The one-stop-shop principle together with the consistency mechanism is one of the central planks of the Commission proposal for a General Data Protection Regulation. It was discussed already three times at the Council (October and December 2013 and June 2014). At the heart of the matter are questions related to the architecture of the data protection supervision of companies active in several Member States.

Current situation

2. Under Directive 95/46/EC, a company operating in more than one Member State may have to deal with several DPAs, but without any guarantee that these DPAs coordinate or cooperate when adopting their positions. The Directive does not provide for any detailed obligation to coordinate or cooperate between the other potentially concerned DPAs (e.g. those from the Member States of the complainants).This situation may result in legal uncertainty for companies and fragmented and inefficient protection for individuals in respect to data processing activities with cross-border impact.

3. As for the data subject, Article 28(4) of the 1995 Directive provides that '[e]ach supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data', means that affected data subject can lodge a complaint at their 'own' supervisory authority. When the processing of a company based in only one Member State affects data subjects in other Member States, only the DPA where the company is established can decide on the processing. This follows from the definition of territorial applicable law (Article 4(1) (a), (b) and (c) of Directive 95/46/EC). That Directive gives as the main criterion to trigger the applicability of national law the fact that 'the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State'. This criterion is thus linked to the presence on the Member State territory of the entity carrying out the processing concerned and not to the data subjects affected.

Commission proposal

4. The Commission proposed that, in order to increase the consistent application of the Regulation, provide legal certainty and reduce administrative burden for such controllers and processors, one single supervisory authority be competent for monitoring the activities of the controller or processor throughout the Union and for taking the related decisions, 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,. The competent authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment.

5. The one-stop-shop principle is linked with the mandatory co-operation between the supervisory authorities through the European Data Protection Board, which is aimed at ensuring the consistent application of this Regulation throughout the Union. The one-stop-shop principle would then be an advantage for business within the internal market, which should have to deal only with one supervisory authority throughout the European Union.

II. Presidency proposal: combining a uniform supervision with proximity

6. At the Council meeting on 5 June 2014, an orientation debate on the one-stop-shop mechanism took place, in which several Member States emphasised the need to ensure a grater degree of proximity to data subjects in the elaboration of the one-stop-shop mechanism. Some Member States also referred to the need to develop the role of the European Data Protection Board in this respect. Further to this, the Presidency has revised the proposal to combine the need for an effective uniform decision-making process (by entrusting the Board with binding powers in limited cases) with effective proximity for citizens.

7. The Presidency proposal provides that, in cross-border cases warranting the involvement of the DPAs of several (possibly all 28) Member States, the decision to be taken via the procedures in the Regulation (either co-operation mechanism between the DPAs involved or the consistency mechanism at the level of the EDPB) will be, following this supranational procedure, a single decision agreed jointly by all DPAs concerned (co-decision). This ensures that all interests at stake will be taken into account by allowing each DPA concerned to defend its views. The Presidency endeavoured to strike a balance between uniform supervision and proximity by providing that this decision, agreed upon jointly by the DPAs, be adopted formally by the lead DPA, which will then ensure its implementation via the main establishment of the controller/processor (pursuant to company law) – except in case the decision arises from a cross-border complaint **and adversely affects the complainant**.

In the latter situation, the decision will be adopted formally by the DPA concerned if such complaint was not granted in full (either because it was rejected, dismissed or granted only with regard to certain claims made by the data subject).Allowing the national DPAs to adopt at Member State level the uniform decision agreed at supranational level thus serves the goal of proximity in a second way. It allows the data subjects affected by the decision to have the decision of national DPA reviewed by the national court of that Member State. Under the Commission's proposal, the decision would be adopted only by the lead authority, thus depriving data subjects residing in a Member State other than that of the lead authority of the possibility to have that decision reviewed by their 'local' court. At the same time it is clear that increasing proximity by multiplying the avenues for judicial review of the single supervisory DPA decision, may create some risks for legal certainty as it may result in contradictory court judgments and even in forum shopping. The Presidency has tried to address, at least in part, these concerns by amending Article 76a in order to better clarify the mechanism leading to suspension of possible co-existing judicial proceedings (see infra Nos xxx) and by recalling the role of the Court of Justice of the European Union in preliminary rulings concerning the interpretation of Union law which precisely aims at providing for a uniform interpretation of Union law and thus avoiding contradictory national judgments (see last sentence of Recital 113).

III. Defining the scope of the one stop-shop mechanism

Scope of the uniform supervisory decision: conformity with the General Data Protection Regulation or also the corrective measures to be applied

8. One of the most important questions surrounding the one-stop shop mechanism, concerns the scope of the single decision that will be agreed upon: (1) is it limited to assessing whether and to what extent a particular type of processing is in conformity or in violation of the Regulation or (2) does it also extend to the follow-up that should be given to any violation, i.e. the corrective measures. The second scenario presumes either that the Regulation would concentrate the power to impose corrective measures in the hands of the lead authority or that all authorities involved would impose the same type of corrective measure for a violation which affected data subjects in several Member States. Whilst agreeing at EU level on corrective measures has an obvious attractiveness to it, there are also important drawbacks to it. In the decision-making process of national DPAs regarding corrective measures to be imposed following a data protection violation, DPAs may take account of many different factors (see paragraph 2a of Article 79), some of which may be proper to the Member State concerned. Moreover the single decision to be agreed upon in the context of the one-stop-shop mechanism cannot take account of relevant Member State legislation, such as, for example, (constitutional) rules on the freedom of expression. This legislation may also play an important role in the determination of which corrective measures to apply. The second scenario under which only the lead authority would adopt the corrective measure seems at any rate excluded for any corrective measure affecting the situation of the data subject (e.g. the rectification or deletion of his/her personal data), as this would deprive him/her of the possibility challenge the decision on corrective measure before his/her local court.

No limitation of the jurisdiction of local DPAs

9. Under the 1995 Data Protection Directive, the territorial scope of application of the Directive is governed by Article 4(1), according to which a Member State, as a rule, is to apply the national provisions it adopts pursuant to the Directive to the processing of personal data where there is an establishment of the controller on its territory[1]. The draft Regulation also enshrines the territorial jurisdiction of that DPA by stating in Article 51(1) that each supervisory authority shall exercise its powers, on the territory of its own Member State. However, for cases falling within the scope of the one-stop-shop mechanism (where the processing takes place in the context of the activities of an establishment of a controller or a processor established in more than one Member State), the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States (Article 51(2)).

10. In the Commission proposal the jurisdiction of the lead authority, that is the authority of the Member State of the main establishment, can be read to be exclusive; the jurisdiction of the lead authority to impose corrective measures deprives the DPA of other Member State where the company has an establishment, of its possibility to exercise these powers regarding that establishment on its territory**, unless the corrective measure concerns a purely local case**.

11. The Presidency does not deem it expedient to limit the jurisdiction of data protection authorities. The proximity principle requires that each data protection authority can exercise the full panoply of its powers regarding processing activities on its territory. In light of the broad view the ECJ has taken of jurisdiction of national data protection authorities and with regard to possible future developments of ECJ case law, it would not appear wise for the legislator to limit the jurisdiction of national data protection authorities. The recent ECJ judgment in the case of Google (C-131/12) implies that, under the 1995 Directive in case of multiple establishments, a data subject can seek redress, including by corrective measures, from the data protection authority of any Member State where the controller has an establishment and not only from the Member State where the controller has its main establishment. The Presidency cannot see any valid ground that would justify curtailing the rights data subjects currently enjoy and thus decrease this level of protection.

[1] Or in cases where the controller is not established in the Union, if he makes use of equipment situated on the territory of the Member State for the purposes of processing personal data.

12. This obviously does not detract from the fact that where the one-stop-shop mechanism is triggered DPAs will not only have the possibility but also the obligation to comply with the outcome of a supranational decision-making procedure.

Local cases: local DPA and local judge

13. While under the one-stop-shop mechanism the DPA of the main establishment shall normally act as lead authority for the entire Union, the draft Regulation provides for an exception where processing activities in the context of an establishment of the controller or company not substantially affect data subjects in other Member States: These cases can continue to be dealt with by the local DPA.

14. This is the case for complaints (e.g. employee data base) or infringements of the Regulation (e.g.: local data breach not related to the security settings decided by the headquarters) with purely local impact. Many cases of day-to-day processing activities are and will continue being local cases. The decisions of local DPAs will be challengeable before the "local" courts.

15. The local DPA has several tools at its disposal:

- it can grant, reject or dismiss a complaint;
- it can seek an amicable settlement between the complainant and the company (Article 52(1), letter b));
- it can exercise the whole range of powers (ex: corrective, authorisation) in respect of the controller (Article 53).

IV. Two supranational procedures for the one stop-shop mechanism

16. The one-stop-shop mechanism should only intervene in important cross-border scenarios. In the Commission proposal this referred to processing in the context of the activities of an establishment of the same controller or processor established on the territory of different Member States. During the discussions in the Working Party, a second type of cases has been included in the scope of the one-stop-shop mechanism, namely processing by a controller or processor established in one Member State, but which affects data subjects in other Member States. Two types of supranational co-operation may take place in order to arrive at a uniform decision for all Member States involved. A first type of co-operation takes place between Member States concerned and allows them to arrive at a common position. Only if the DPAs involved do not agree, will the matter be forwarded to the Board for resolution (consistency mechanism).

Co-decision: lead DPA and DPAs concerned jointly agree on a single supervisory decision

17. The single supervisory decision (Article 54a (4**a**)) must be based on an agreement by all DPAs concerned: the DPAs of the complainants, the DPA of the main establishment and the DPAs of the other establishments. Having agreed on this single decision jointly, all DPAs concerned (and the lead DPA) will be bound by it.

18. In cross-border cases the lead DPA, which acts as supervisory authority, proposes the single supervisory decision. The proximity, of which the importance was emphasised repeatedly at the Council, is ensured by the involvement of the local supervisory authorities in the decision-making process by the lead DPA. A second element of proximity is that each authority retains jurisdiction in cases affecting individuals within its territory. In case the decision arises from a complaint (or several complaints) having a cross-border dimension, the 'local' authority will have the possibility to adopt formally the decision agreed upon jointly with the lead authority and therefore notify it to the complainant and/or enforce it locally if that decision affects the complainant – because it did not grant the complaint in full (rejected it, dismissed it, granted it only in part) (Article 54a (4**b**)).

19. All concerned DPAs will be in a position to intervene in all stages of the one-stop-shop decision-making process and must jointly agree on the supervisory decision (co-decision model). Where a DPA other than the lead authority objects and the lead DPA does not endorse such objection, this triggers the intervention of the European Data Protection Board (Article 57).

20. The Presidency has thus tried to increase the proximity of the decision-making process and to accommodate a key criticisms regarding the one stop-shop mechanism, i.e. a perceived transfer of powers and the need to enforce decisions of another Member State.

21. The DPAs of the complainants will inform the complainant about the outcome of his/her request providing details about the procedure followed and the decision adopted jointly with ~~of~~ the lead DPA (Article 54a(4a). In case of failure to act of the lead DPA, the local DPA can also adopt either a provisional measure in case of mutual assistance or, in exceptional circumstances, adopt provisional measures intended to produce legal effects (Article 61).

Consistency mechanism: the European data Protection Board adopts binding decisions in case of dispute resolution

22. Several Member States have called for the Board being entrusted with binding powers in specific cases. The Presidency considers that binding powers of the Board appear to be suitable for dispute resolution in three different type of conflictual cases (Article 57(2a)):

- conflicts as to the identification of the lead DPA;
- conflicts as to the functioning of cooperation between DPAs (mutual assistance, joint operations cases);
- conflicts as to the merits of the case (objections to a draft decision of the lead DPA, failure to act by the lead DPA).

23. In the dispute resolution model, the decision of the Board would be binding on the DPAs concerned. On this basis, the lead DPA would adopt and serve the substantive decision on the main establishment of the controller. The DPAs of the complainants will also inform the complainants about the outcome of the decision adopted by the Board.

24. The Presidency has added an Article (58a) empowering the Board to take such binding decisions and has tried to clarify the relevant procedural arrangements in another Article (Article 68). Furthermore, the Presidency has endeavoured to provide a possible layout for the Board as a Union body having legal personality; to that end, Article 64 was amended accordingly whilst the list of the tasks of the Board was also expanded to reflect the proposed configuration (Article 66). Undoubtedly further drafting will be required in this regard.

V. Judicial review and judicial redress

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

26. *Judicial review* is closely linked to the power of the supervisory authority of that Member State and should therefore be possible only in the courts of the Member State of the supervisory authority concerned. Under Article 73(1) data subjects would have the right to lodge a complaint with a supervisory authority in any Member State. This would leave, as it is currently the case under the 1995 Data Protection Directive, supervisory authorities the competence to hear complaints by data subjects and data subjects to decide where they want to go.

27. In the view of the Presidency, it is a crucial element of proximity that the decisions of the lead DPA and of other supervisory authorities, which will have agreed to adopt an identical decision, should be challengeable before the courts of the Member States concerned whenever they affect data subjects. In this sense, the Presidency proposal that in all such cases all concerned DPAs adopt an identical decision is an essential element of the one-stop shop mechanism, because it guarantees that all affected data subjects will have the possibility to challenge the DPA decision before their local court.

28. In the Presidency's draft, this is not only true for cases where there is agreement between the DPAs involved (co-decision), but also in cases where the EDPB has taken a decision, as this decision will be binding in its entirety on the lead and other supervisory authorities concerned, which will have to give effect to the EDPB decision at national level. In this way, the Presidency has endeavoured to address one of the main weaknesses of the Commission proposal for the one-stop shop mechanism. It has previously been demonstrated that there were limits to the degree to which proximity can be ensured regarding judicial review in those cases where the supervisory authority of the main establishment would have the exclusive power to adopt corrective measures. In such a case only the courts of the main establishment Member State would have jurisdiction, not those of other Member States whose data subjects are affected and where they may have lodged a complaint. In the current Presidency draft also those data subjects will have the possibility to have the DPA decision reviewed.

29. The Presidency draft, however, also allows data subjects and controllers to challenge the EDPB decision directly before the ECJ[2] by way of an action for annulment[3] (Article 76b, new). The failure to do so will, however, not deprive the data subject of his remedy before national courts as he may still call in question the lawfulness of the EDPB decision later on in the context of the judicial review of the DPA decision which gives effect to the EPDB decision. When a court of a Member State is asked to review the decision of the DPA of that Member State which gives effect to an EDPB decision, that court shall request the ECJ for a preliminary ruling on the validity of that EDPB decision but only when that national court considers that EDPB decision may be invalid.

30. Regarding *judicial redress*, Article 75 provides that proceedings shall be brought before the courts of the Member State where the controller or processor has an establishment. It has been established that the general rules on jurisdiction (in particular those flowing from the Brussels I Regulation) provide sufficient grounds of jurisdiction for the courts of the Member state to order measures against the controller or processor responsible for the alleged data protection violation. The articulation of the provisions on jurisdiction in this Regulation with the Brussels I Regulation is clarified in recital 118a.

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

---

[2] It will actually be the General Court of the European Union in accordance with the EU jurisdictional rules.

[3] See the first and fifth paragraphs of Article 263 TFEU on actions for annulment against acts adopted by Union bodies and intended to produce legal effects.

ANNEX

16a) *While this Regulation applies also to the activities of courts* and other judicial authorities, Union or Member State law could **(…),** specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. *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 the judiciary in the performance of its judicial tasks, **including its decision-making**. Supervision of such data processing operations may be entrusted to specific bodies within the judicial system of the Member State, which should in particular control compliance with the rules of this Regulation, promote the awareness of the judiciary of their obligations under this Regulation and deal with complaints in relation to such processing.

(…)

95a) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, processing affecting data subjects on its territory or processing carried out by a controller not established in the European Union when targeting data subjects residing in its territory. This should include dealing with complaints lodged by a data subject, conducting investigations on the application of the Regulation, promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

96) 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, this Regulation should oblige and empower the supervisory authorities to co-operate with each other and the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

96a) Where the processing of personal data *takes place* in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State**,** or where processing **taking place in the context of the activities of a single establishment of a controller or processor in the Union** substantially affects or is likely to affect substantially data subjects in more than one Member State, **the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor** should act as lead authority. Within its tasks to issue guidelines on any question covering the application of this Regulation, the European Data Protection Board may issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State.

(…)

The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities and bodies of a Member State. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or body is established.

96b) The lead authority should be competent to decide on measures applying the powers conferred on it in accordance with the provisions of this Regulation. In its capacity as lead authority, the supervisory authority should closely involve **and coordinate** the supervisory authorities concerned in the decision-making process.

96c) The decision of the lead **authority should be taken jointly with the other supervisory authorities concerned and** should be directed towards the main **or single** establishment of the controller or processor and be binding **on** the controller and processor. The controller or processor should take the necessary measures to ensure the compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the context of all its establishments in the Union.

100) 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 tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, particularly in cases of complaints from individuals, and to bring infringements of this Regulation to the attention of the judicial authorities and/or engage in legal proceedings. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities (…) should be exercised in conformity with appropriate procedural safeguards set out in Union law and national law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in national procedural law, such as the requirement to obtain a prior judicial authorisation.

Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head or a member of the supervisory authority of a person authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to national procedural law.

100a)**(…)**

101) **(…)**[4].

[4] Moved to recital 111.

101) Where the supervisory authority to which the complaint has been lodged is not the **lead** supervisory authority, the **lead** 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 **lead** 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.

101a) The supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible **infringements of the Regulation** should seek an amicable settlement **and, if this proves unsuccessful, exercise its full range of powers** in cases where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint **o**r the possible **infringement** concerns only processing activities of an establishment of the controller or processor in the one single Member State where the complaint has been lodged or the possible **infringement** detected and the matter does not **substantially** affect **(…)** data subjects **in other Member States**.

102) 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.

103) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. Where a supervisory authority requesting mutual assistance, in the case of no response of the requested supervisory authority within one month of receiving the request, adopts a provisional measure, such provisional measure should be duly justified and only of a temporary nature.

104) 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.

104a)(…)[5]

105) 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 adopt a measure intended to produce legal effects 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.

106) 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. **The European Data Protection Board should also be empowered to issue binding decisions in cases where there are conflicting views among supervisory authorities with a view to taking measures that are intended to produce legal effects in several Member States.**

107) (…)

108) 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.

[5] Merged with recital 110.

109) The application of this mechanism should be a condition for the (…) lawfulness of a (…) measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the consultation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and 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.

110) **In order to promote the consistent application of this Regulation, the European Data Protection Board should be set up as an independent body of the Union. To fulfil its objectives, the European Data Protection Board should have legal personality. The European Data Protection Board should be represented by its Chairperson.** 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 **or his or her representative** 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, in particular on the level of protection in third countries or international organisations, 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, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. **Each supervisory authority to which a complaint has been lodged should deal with the complaint and should investigate the matter to the extent appropriate. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can be completed also electronically, without excluding other means of communication.**

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[6]**.**

112) Where a data subject considers that his or her 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.

[6] Moved from Recital 101.

113) Without prejudice to the right of natural or legal person to bring an action for annulment of decisions of the European Data Protection Board which have been notified to him or her before the Court of Justice of the European Union, each natural or legal person should have the right to an effective judicial remedy against a decision of a supervisory authority which produces legal effects concerning this person. Such decisions concern in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, this right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. The fact that a natural or legal person has not brought an action for the annulment of the European Data Protection Board's decisions before the Court of Justice of the European Union within the mandatory time-limit, does not bar that person from calling in question the lawfulness of that decision before the national courts at a later stage in particular in the context of judicial review of a supervisory authority's decision applying the European Data Protection Board's decision. In that context, where a national court considers that the European Data Protection Board's decision may be unlawful, it shall request the Court of Justice of the European Union a preliminary ruling concerning the validity of that European Data Protection Board's decision, in accordance with Article 267 TFEU as interpreted by the Court of Justice in the *Foto-frost* case[7]. 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 procedural 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. Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings to **the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts whose decisions may be subject to appeal under national law should endeavour to request a preliminary ruling concerning the interpretation of Union law including this Regulation, in particular where the case involves a data subject who has lodged a complaint with a supervisory authority located in a Member State other than the one where the controller or processor has its establishment.**

[7] Case C-314/85.

113a) Where a court seized with a proceeding against a decision of a supervisory authority has reason to believe that proceedings concerning the same processing activities or the same cause of action are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seised should stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if the latter has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings.

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[8].

[8] COM scrutiny reservation.

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[9].

[9] COM and DE scrutiny reservation.

SECTION 2

COMPETENCE, TASKS AND POWERS

Article 51

Competence [10] [11]

1. Each supervisory authority shall (…) be competent on the territory of its own Member State to (…) perform the tasks and to exercise the powers conferred on it in accordance with this Regulation (….)[12].

a) (….)

b) (…..)

c) (….)

[10] COM reservation. Scrutiny reservation on the one-stop-shop mechanism by DE, DK, EE, FR, MT, NL, PT, RO and UK. Some delegations (BG, CY, DE, GR, NL and LU) supported one-stop-shop principle, but had many questions of understanding as to its practical implementation. Other delegations (BE, CZ, ES, FR, HU, IT, AT, PT, RO and SI) had a more critical attitude and entered a reservation. Several referred to the problem of proximity. 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). In this regard the issue of divergent MS case law was mentioned. 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.

[11] NL thought all jurisdiction rules should be set out in this article, covering both domestic and cross-border cases and private as well as public controllers (and processors). 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.

[12] DK, DE and EE queried whether the decisions of this DPA would also be binding on controllers outside that MS. Constitutional reservation by DK.

1a. ***Each supervisory authority shall be competent to deal with a complaint lodged in accordance with Article 73(1), or to deal with a possible infringement of this Regulation detected by or otherwise brought to its attention, including for seeking an amicable settlement of the complaint or infringement case and by exercising all the powers conferred on it pursuant to Article 53, unless the case concerns processing activities in the context of more than one establishment of a controller or processor who is established in more than one Member State or data subjects in other Member States are substantially affected by the processing in question pursuant to Article 51a(1).***

1b. (…)

1c. (…)

2. (…)

2a. (…)

2b. (…)

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity[13]. Supervision of such processing operations may be entrusted to specific bodies, which form part of the judiciary and are designated by the law of the Member State.

[13] 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.

Article 51a

Competence of the lead supervisory authority

1. Without prejudice to Article 51, where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State**,** or where the processing of personal data takes place in the context of the activities of a single establishment of a controller or processor in the Union and the processing substantially affects or is likely to affect substantially data subjects in more than one Member State, the supervisory authority for the main establishment or for the single establishment of the controller or the processor shall act as lead supervisory authority and shall be competent for decisions pursuant to (…)[14] paragraphs 1, 1b and 1c of Article 53 against such controller or processor in accordance with the procedure foreseen in Article 54a **(…).**

1a. (…)[15]

2. (…)

3. **(…)**

4. **This** article shall not apply where the processing is carried out by public authorities and bodies of a Member State.

[14] NL scrutiny reservation.
[15] Moved to Article 51(1a).

Article 51b

Identification of the supervisory authority competent for the main establishment

1. Any controller or processor which carries out processing of personal data in the context of the activities of an establishment in the Union and is established in more than one Member State shall indicate to the supervisory **authorities concerned** where its main establishment is located (…).

1a. When indicating its main establishment pursuant to paragraph 1, the controller or processor shall list all its establishments in the Union for which the decisions on the purposes and means of processing are taken at the main establishment and shall, on the request of any supervisory authority **concerned**, provide further information in relation to the existence of the main establishment in the place specified. The controller or processor shall inform the supervisory authorities **concerned** on any changes of the information provided.

1b. The supervisory authority **of the main establishment indicated as per paragraph 1 shall verify the existence of the main establishment at the place specified and notify the outcome of its verification to the controller or processor, the other supervisory authorities concerned and** the European Data Protection Board.

2. Where there are conflicting views between the supervisory authorities concerned on which supervisory authority is (….) that for the main establishment, any of the supervisory authorities concerned may refer the matter to the European Data Protection Board. The European Data Protection Board shall issue **decision** on the identification of the supervisory authority for the main establishment in accordance with **the procedure provided for in** Article 58a.

Article 51c

One-stop shop register[16]

The European Data Protection Board shall keep a public register **of the verified** information referred to in paragraph **(…).** 1a of Article 51b for consultation, which shall be electronically accessible to anyone free of charge.

Article 52

Tasks [17]

1. Without prejudice to other tasks set out under this Regulation[18], each supervisory authority shall on its territory[19]:

(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) advise, in accordance with national law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data[20];

---

16 ES remarked that this would be very costly

17 DE, IT, AT, PT and SE scrutiny reservation. UK thinks the term 'functions' rather than 'duties' should be used.

18 New text as paragraphs (f) to (i) have been deleted as these duties were already laid down elsewhere in the Regulation.

19 A recital should be drafted 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.

20 NL reservation.

(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;

(b) deal with complaints[21] lodged by a data subject, or body, organisation or association representing a data subject in accordance with Article 73[22], 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[23] , in particular if further investigation or coordination with another supervisory authority is necessary;

(c) cooperate with, including sharing information, 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, including on the basis of ~~a~~ information received from another supervisory or other public authority, or in response to a complaint;

(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;

---

21 IT scrutiny reservation on the term complaint; UK thought the emphasis should be on complaint-resolution.

22 BE suggested limiting this to the data subject itself.

23 IT suggested fixing a 10-weeks period for dealing with the complaint.

(f) adopt standard contractual clauses referred to in Article 26(2c);

(fa) establish and make a list in relation to the requirement for data protection impact assessment pursuant to Article 33(2a);

(g) give advice on the processing operations referred to in Article 34(3) **(…)**[24] ;

(ga) encourage the drawing up of codes of conduct pursuant to Article 38;

(gb) promote the establishment of data protection certification mechanisms and of data protection seals and marks;

(gc) **where applicable,** carry out a periodic review of certifications issued in accordance with Article 39(4);

(gd) (…);

(h) **draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 38a and of a certification body pursuant to Article 39a;**

(ha) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 38a and of a certification body pursuant to Article 39a;

(hb) authorise contractual clauses referred to in Article 42(2)(d);

(i) approve binding corporate rules pursuant to Article 43;

(j) contribute to the activities of the European Data Protection Board;

(k) fulfil any other tasks related to the protection of personal data.

2. (…).

3. (…).

[24] Deleted as it is already in Article 53(1c)(ab).

4. Each supervisory authority shall facilitate the submission of complaints referred to in point (b) of paragraph 1, by measures such as providing a complaint submission form which can be completed also electronically, without excluding other means of communication.

5. The performance of the tasks 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[25]. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request[26].

[25] 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.

[26] DE, NL and SE reservation: this could be left to general rules.

Article 53

Powers[27] [28]

1. Each Member State shall provide by law that its supervisory authority shall have at least[29] the following investigative powers:

(a) to order the controller and the processor[30], and, where applicable, the controller's representative to provide any information it requires for the performance of its duties;

(aa) to carry out investigations in the form of data protection audits[31];

---

27 DE, NL, RO, PT and SE scrutiny reservation; SE thought this list was too broad. Some Member States were uncertain (CZ, RO and UK) or opposed (DE, DK, NL and IE) to categorising the DPA powers according to their nature. DK has raised serious constitutional concerns -based on the understanding that a decision by a "lead authority" in one Member State would be directly binding for the concerned establishments in all Member States. There is no problem if there were to be no doubt that a decision by the "lead authority" should be directed towards the "main establishment" and should *only* be binding for this establishment. It would then be for the "main establishment" – e.g. through internal business/cooperation rules – to implement the decision in subsidiaries in other Member States. If it is the case that a decision by a "lead authority" in another Member State is not to be binding for e.g. an establishment in Denmark, Denmark will not have a constitutional problem with the one-stop-shop principle. In this case the principle would not entail the transfer of powers from Danish authorities to authorities in other Member States.

28 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.

29 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.

30 NL thought that all the powers listed in para. 1 should also be available vis-à-vis others than controllers and processors.

31 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 current drafting does not preclude this.

(ab) to carry out a review on certifications issued pursuant to Article 39(4);

(b) (…)

(c) (…)

(d) to notify the controller or the processor of an alleged infringement of this Regulation[32] (…);

(da) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its duties;

(db) to obtain access to any premises of the controller and the processor , including to any data processing equipment and means, in conformity with Union law or Member State procedural law.

1a. (…).

[32] BE suggested adding the power to oblige the controller to communicate the personal data breach to the data subject.

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[33] to a controller or processor where processing operations have infringed provisions of this Regulation[34];

(c) (…);

(ca) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation[35];

(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; in particular by ordering the rectification, restriction or erasure of data pursuant to Articles 16, 17 and 17a and the notification of such actions to recipients to whom the data have been disclosed pursuant to Articles 17(2a) and 17b;

(e) to impose a temporary or definitive limitation on processing[36];

(f) to order the suspension of data flows to a recipient in a third country or to an international organisation[37];

(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.

---

33 EE, IT, PL, SE and SK scrutiny reservation.

34 PL scrutiny reservation on points (a) and (b).

35 NL queried whether it would possible to impose penalties in case of non-compliance (*astreinte/dwangsom*).

36 NL scrutiny reservation. The word' limitation' may accommodate concerns relating to the compatibility with the freedom of expression.

37 SK reservation.

1c. Each Member State shall provide by law that its supervisory authority shall have the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 34[38],

(aa) to issue, on **its** own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, or, in accordance with national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(ab) to authorise processing referred to in Article 34(7a);

(ac) to issue an opinion and adopt draft codes of conduct pursuant to Article 38(2);

(ad) to accredit certification bodies under the terms of Article 39a;

(b) authorise standard data protection clauses referred to in point (c) of Article 42(2);

(c) authorise contractual clauses referred to in point (d) of Article 42(2);

(d) approve binding corporate rules pursuant to Article 43.

2. *The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter of Fundamental Rights of the European Union.*[39]

---

38 NL scrutiny reservation. This was placed in the wrong category.

39 CY, ES, FR, IT and RO thought this could be put in a recital as these obligations were binding upon the Member States at any rate. COM could accept this.

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 and/or, where appropriate, to commence or engage otherwise in legal proceedings[40], in order to enforce the provisions of this Regulation[41].

4. (…)

5. (…)

Article 54

Activity Report

Each supervisory authority shall draw up an annual report of its activities. The report shall be transmitted to the national Parliament, the government and other authorities as designated by national law. It shall be made available to the public, the European Commission and the European Data Protection Board.

[40] 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.

[41] DE thought para. 3 and 4 should be deleted.

CHAPTER VII[42]

CO-OPERATION AND CONSISTENCY

SECTION 1

CO-OPERATION

Article 54a

Cooperation between the lead supervisory authority and other supervisory authorities concerned[43]

1. In the cases referred to in paragraph 1 of Article 51a, (….) the lead supervisory authority (…) shall cooperate with the supervisory authorities concerned in accordance with this article **(…)** in an endeavour to reach consensus (…). (…)

1a. In the cases referred to in paragraph 1 of Article 51a, each supervisory authority concerned shall inform the lead supervisory authority and refer the matter to the lead supervisory authority **(…).**.

2. (…) The lead supervisory authority shall, without delay, further investigate the subject matter and communicate the relevant information on the matter to the supervisory authorities concerned and shall**(…).** submit a draft decision on such measure to all supervisory authorities concerned for their opinion and take due account of the views of those supervisory authorities.

a) (…)

b) (…)

c) (…)

---

42 AT and FR scrutiny reservation on Chapter VII.

43 BE, CZ, CY, DE, EE, FR, FI, IE, LU, RO, PT and NL scrutiny reservation. IE pointed out that in the case of personal data processed by social media or other internet platforms, all 28 MS DPAs would be 'concerned'. LU and NL doubted that one DPA concerned would be sufficient to trigger the consistency mechanisms. BE, FR, PL and LU expressed a preference for amicable settlements.

2a. (…)

2b. The lead supervisory authority may request at any time other concerned supervisory authorities to provide mutual assistance pursuant to Article 55 **and may conduct joint operations pursuant to Article 56**, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. Where any of the supervisory authorities concerned expresses a reasoned objection within a period of four weeks after having been consulted in accordance with paragraph 2 **to** the draft decision, the lead supervisory authority shall**, if it does not follow the objection,** submit the matter to the consistency mechanism referred to in Article 57. **In such a case, the decision adopted accordingly by the European Data Protection Board shall settle the case and be binding on the lead supervisory authority and all the supervisory authorities concerned pursuant to point 2(a) of Article 57 and Article 58a.** Where a supervisory authority concerned has not objected within this period, it is deemed to be in agreement with the draft decision.

4. Where no supervisory authority concerned has objected to the draft decision submitted by the lead supervisory authority **within the period referred to in paragraph 3,** the lead supervisory authority and the supervisory authorities concerned shall **agree on a single** decision **jointly.**

4a. The lead supervisory authority shall **adopt the decision and notify it** to the main establishment or single establishment of the controller or processor on the territory of its Member State and inform the European Data Protection Board of the decision in question **including a summary of the relevant facts and grounds.**

4~~a~~b. Where the decision jointly agreed upon concerns a complaint and as far as it adversely affects the complainant, notably where the complaint is rejected, dismissed or granted only in part, each supervisory authority that have received such complaint shall adopt the single decision concerning that complaint and serve it on the complainant. The complainant shall be informed in any case of the outcome of the complaint pursuant to Article 73, paragraph 5.

4c. **After being notified of the decision of the lead supervisory authority pursuant to paragraph 4a,** the controller or processor shall take the necessary measures to ensure compliance with the decision as regards the processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall then inform all the supervisory authorities concerned. The supervisory authorities concerned shall be bound by the single decision adopted jointly in the manner described above. ~~W~~

4. (.)

4a. (.)

4d. Where, in exceptional circumstances, a supervisory authority **concerned** has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 61 shall apply.

5. The lead supervisory authority and the supervisory authorities concerned shall supply the information required under this Article **(…)** to each other by electronic means, using a standardised format.

Article 54b

Cooperation ***between the lead supervisory authority and the other supervisory authorities concerned in individual cases of possible non-compliance with the Regulation***

(…)

Article 55

Mutual assistance[44]

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. (...)

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[45] after having received the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation (…).

3. The request for assistance shall contain all the necessary information[46], 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.

---

44 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.

45 ES had suggested reducing 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.

46 EE and SE scrutiny reservation.

4. [47]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[48]; 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[49].

6. Supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means[50], 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[51].

---

47 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.

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

49 RO scrutiny reservation.

50 PT (supported by RO) suggested adding "or other means if for some reason, electronic means are not available, and the communication is urgent".

51 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 of another supervisory authority, the requesting supervisory authority may adopt a provisional measure[52] 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[53].

9. The supervisory authority shall specify the period of validity of such a provisional measure which shall not exceed three months[54]. 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)[55].

---

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

53 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.

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

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

Article 56

Joint operations of supervisory authorities[56]

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 [57]] data subjects in more than one Member State 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[58] authority shall invite the supervisory authority of each of those Member States to take part in the joint operations concerned and respond without delay to the request of a supervisory authority to participate[59].

---

56 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 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.

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

58 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.

59 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 law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. (…) [60]

3a. Where, in accordance with paragraph 1, staff of a seconding supervisory authority are operating in another Member State, the Member State of the host 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 seconding supervisory authority whose staff has 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 (…) 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[61].

4. (…)

---

60 DE, LU, PT and COM scrutiny reservation on the deletion of this last phrase.

61 Inspired by Article 3 of the Council Framework Decision of 13 June 2002 on joint investigation teams. UK reservation on paras. 3a, 3b and 3c.

5. [62]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.

62 NL asked whether the measures of paragraphs 5 and 6 were really necessary. EE suggested a merger of the two paragraphs.

SECTION 2

CONSISTENCY[63]

Article 57

Consistency mechanism[64]

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[65].

1a. (…)

1b. (…)

2. The European Data Protection Board shall **(…)** issue an opinion whenever a competent *supervisory authority* intends *to adopt* any of the measures below and such measures may produce effects in more than one Member State. To that end, the competent supervisory authority shall communicate the draft measure to the European Data Protection Board, 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

---

63 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.

64 EE, FI, LU, NL and UK scrutiny reservation.

65 CZ, DE, ES and RO 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.

(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

(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.

2a. The European Data Protection Board shall **(…)** adopt a binding decision in the following cases:

a) Where, in a case referred to in paragraph 3 of Article 54a(…), a supervisory authority concerned (…) expresses a reasoned objection to a draft measure. In that case, the lead supervisory authority shall communicate the matter to the European Data Protection Board in order for the Board to definitively settle the conflicting views on the draft measure;

b) Where, in a case referred to in paragraph 2 of Article 51b, there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment. In that case, any of the supervisory authorities concerned may communicate the matter to the European Data Protection Board (…);

c) Where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56. In that case, any supervisory authority concerned[66], the **lead supervisory authority** or the Commission may communicate such matter to the European Data Protection Board[67];

d) Where a competent supervisory authority does not request the opinion of the European Data Protection Board in the cases mentioned in paragraph 2 of this Article, or does not intend to follow the opinion of the European Data Protection Board issued as per Article 58. In that case, any supervisory authority concerned, the **lead supervisory authority** or the Commission may communicate the matter to the European Data Protection Board.

[2b. The lead supervisory authority shall inform the European Data Protection Board within three weeks of any measure adopted pursuant to Article 54a(4**a**) and also provide a summary of the facts and grounds that made the taking of such measure necessary.]

2c. Any supervisory authority (…), the Chair of the European Data Protection Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the European Data Protection Board with a view to obtaining an opinion.

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.

---

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

67 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.

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.

Article 58

Opinion by the European Data Protection Board[68]

1. (…)

2. (…)

3. (…)

4. (…)

5. (…)

6. (…)

6a. (…)

7. In the cases referred to in paragraphs 2 and 2c of Article 57, the European Data Protection Board shall issue an opinion on the subject- matter submitted to it provided it has not already issued an opinion on the same matter[69]. This opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. This period may be extended by a further month, taking into account the complexity of the subject matter. Regarding the draft decision 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 decision.

---

68 NL and UK scrutiny reservation.

69 ES suggested keeping the possibility for one DPA requesting an opinion from the EDPB.

7a. Within the period referred to in paragraph 7 the competent supervisory authority shall not adopt its draft measure as per paragraph 2 of Article 57.

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 2 and 2c of Article 57 and the Commission of the opinion and make it public.

8. The supervisory authority referred to in paragraph 2 of Article 57 shall take utmost account of the opinion of the European Data Protection Board and shall within two weeks after receiving the opinion, electronically communicate to the chair of the European Data Protection Board whether it maintains or will amend its draft measure and, if any, the amended draft measure, using a standardised format.

9. Where the supervisory authority concerned informs the chair of the European Data Protection Board within the period referred to in paragraph 8 that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, paragraph 2a of Article 57 shall apply.

10. (…)

11. (…)

Article 58a

Decisions by the European Data Protection Board

1. In the cases referred to in paragraph 2a of Article 57, the European Data Protection Board shall adopt a decision on the subject-matter submitted to it in order to ensure the correct application of this Regulation in individual cases.
2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-third majority of the members of the **European Data Protection** Board. **The absence of any response shall not be deemed to signify agreement with the decision.** This period may be extended by a further month on account of the complexity of the subject-matter.
3. The supervisory authorities concerned and the lead authority, as the case may be, may not adopt a decision on the subject-matter submitted to the Board under paragraph 1 during the period referred to in paragraph 2.
4. The decision referred to in paragraph 1 shall state the underlying reasons.
5. The decision referred to in paragraph 1 shall be binding in its entirety and addressed on the supervisory authorities concerned and the lead authority, as the case may be.
6. The Chair of the European Data Protection Board shall notify, without undue delay, the decision referred to in paragraph 1 **to** the supervisory authorities concerned and the lead authority **(…)** as well as, where applicable, the complainant(s)[70]. It shall inform the Commission thereof.
7. [The supervisory authorities concerned shall, on the basis of the decision referred to in paragraph 1, without undue delay and at the latest by one month after service of such decision, adopt their final decision on the specific subject-matter under the terms of Article 54, paragraph 4**a**.]

[70] IE asked whether the Chair would notify this directly to the complainant.

Article 59

Opinion by the Commission[71]

(…)

Article 60

Suspension of a draft measure[72]

(…)

Article 61

Urgency procedure[73]

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 intended to produce legal effects (…) for the territory of its own Member State[74], 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[75].

---

71 Deleted in accordance with the request from BE, CZ, DE, ES, SE and UK. COM and FR reservation on deletion.

72 Deleted at the suggestion of BE, CZ, DE, ES, IT, SE and UK. PT scrutiny reservation. COM and FR reservation on deletion.

73 DE scrutiny reservation. COM explained that he 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.

74 COM scrutiny reservation.

75 The conditions under which the EDPB needed to be informed also gave rise to questions (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 or an urgent binding decision from the European Data Protection Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the European Data Protection Board 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 or decision, including for the urgent need to act.

4. By derogation from paragraph 7 of Article 58 and paragraph 2 of Article 58a, an urgent opinion or an urgent decision 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) (…)[76]

(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).

[76] COM reservation on deletion.

2. (…)

3. (…)

Article 63

Implementation of measures adopted by way of the consistency mechanism[77]

(…)

[77] Deleted further to EE and SI reservation and DE and DK scrutiny reservation.

SECTION 3

EUROPEAN DATA PROTECTION BOARD[78]

Article 64

European Data Protection Board[79]

1a. The European Data Protection Board is established as body of the Union and shall have legal personality.

1b. The European Data Protection Board shall be represented by its Chair**.**

2. The European Data Protection Board shall be composed of the head[80] of one supervisory authority of each Member State **or his/her representative** and of the European Data Protection Supervisor[81].

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[82] 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.

---

78 Several Member States (BE, DE, HR, 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.

79 The term 'Board' seems inappropriate and could be replaced by Committee.

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

81 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.

82 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 or exercising its powers pursuant to Articles 66, 66a and 67.[83]

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 or the exercise of its powers, neither seek nor take instructions from anybody[84].

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:

(aa) monitor and ensure the correct application of this Regulation in the cases provided for in Article 57(2a) **without prejudice to the tasks of national supervisory authorities;**

(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 or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(ba) draw up guidelines for supervisory authorities concerning the application of measures referred to in paragraph 1, 1b and 1c of Article 53 and the fixing of administrative fines pursuant to Articles 79 and 79a[85];

---

83 UK and SI scrutiny reservation.

84 DE scrutiny reservation.

85 DK reservation on the introduction of administrative fines in the text and meant that it was for national authorities to decide on that.

(c) review the practical application of the guidelines, recommendations and best practices referred to in points (b) and (ba);

(ca) encourage 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;

(caa) carry out the accreditation of certification bodies and its periodic review pursuant to Article 39a and maintain a public register of accredited bodies pursuant to paragraph 6 of Article 39a and of the accredited controllers or processors established in third countries pursuant to paragraph 4 of Article 39[86];

(cab) specify the requirements mentioned in paragraph 3 of Article 39a with a view to the accreditation of certification bodies under Article 39;

(cb) give the Commission an opinion on the level of protection in third countries or international organisations, in particular in the cases referred to in Article 41;

(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to **in paragraph 2 and 2c of 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;

(h) maintain a publicly accessible electronic register for consultation on confirmed main establishments referred to in Article 51c;

(i) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues dealt with in the consistency mechanism.

[86] HU said that paragraphs (caa) and (cab) were contrary to the text of the general approach reached in June 2014 (11028/14); it is for the national supervisory authority to do this.

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.

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) as well as of the decisions referred to in paragraph 1 of Article 66a.

Article 68

Procedure

1. The European Data Protection Board shall adopt the decisions[87] referred to in paragraph 1 of Article 58a by a two-third majority of its members**. As regards decisions related to the tasks listed in Article 66 hereof, they shall be taken 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[88].

[87] Some delegations suggested replacing this term that could give rise to confusion, with another, such as for instance "resolution". COM would consider an alternative.

[88] CZ asked with what majority the rules of procedure would be taken.

Article 69

Chair

1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members (…).[89]

2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable once[90].

Article 70

Tasks of the chair

1. The chair shall have the following tasks[91]:

   (a) to convene the meetings of the European Data Protection Board and prepare its agenda;

   (aa) to notify decisions adopted by the European Data Protection Board **to** the supervisory authorities concerned and, where applicable, to the complainant(s) pursuant to Article 58a;

   (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.

---

89 COM found this problematic and maintained its reservation on deletion.

90 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.

91 BE suggesting adding another task, namely the chair's role towards the exterior.

Article 71

Secretariat

1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat[92].

2. The secretariat shall provide analytical, administrative and logistical support to the European Data Protection Board.

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, decisions and other texts adopted by the European Data Protection Board.

[92] 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.

Article 72

Confidentiality[93]

1. The discussions[94] 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.

[93] 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. 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.

[94] 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[95]

Article 73

Right to lodge a complaint with a supervisory authority[96]

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a single supervisory authority, in particular[97] in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her does not comply with this Regulation[98].

1a. (….)

2. (…)

3. (…)

4. (…)

5. The supervisory authority to which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant Article 74[99] or, as regards decisions taken by the European Data Protection Board pursuant to Article 76b.

---

95 AT, FR, EE, ES and RO scrutiny reservation.

96 BE, CY, CZ, EE, IE, LY, PT and SI scrutiny reservation.

97 COM, 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.

98 DE, supported by NL, suggested adding "when its rights are not being respected".

99 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).

Article 74

Right to a judicial remedy against a supervisory authority[100]

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 legally binding decision of a supervisory authority concerning them, (...)[101].

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[102] 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[103] on the progress or outcome of the complaint lodged under Article 73[104].

3. Proceedings against a (…) supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established[105].

3a. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or decision of the European Data Protection Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

4. (…)

5. (…)[106]

---

100 ES, PT and SI reservation. EE, IT and UK scrutiny reservation.

101 DE, supported by IE and SE, suggested adding: 'by which it is adversely affected'.

102 COM reservation.

103 SI indicated that under its law the DPA was obliged to reply within two months.

104 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.

105 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.

106 COM reservation on deletion of paragraphs 4 and 5. DE scrutiny reservation on deletion of paragraphs 4 and 5.

Article 75

Right to a judicial remedy against a controller or processor[107]

1. Without prejudice to any available administrative or non-judicial remedy[108], 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[109] if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment (…)[110]. 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 or processor is a public authority acting in the exercise of its public powers.

3. (…)

4. (…)

---

107 DE, EE, PL, PT, SI and SK scrutiny reservation. ES, IT reservation.

108 SI wanted to delete *non-judicial remedy.*

109 ES asked how judicial remedy would be interpreted and how a missed deadline or that there will be no judicial review would be considered.

110 In view of the concerns raised, the reference to national law has been kept only in recital 113.

Article 76 [111]

Representation of data subjects

1. The data subject shall have the right to mandate a body, organisation or association, *which has been properly constituted according to the law of a Member State and whose statutory objectives include the protection of data subjects' rights and freedoms with regard to the protection of their personal data,*[112] *to lodge the complaint on his or her behalf* [113] and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf[114].

1a. [Independently of a data subject's mandate or complaint, any body, organisation or association referred to in paragraph 1[115] shall have the right to lodge a complaint with the supervisory authority competent in accordance with Article 51[116] 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.[117]].

---

111 DE, ES, PT, RO and SI scrutiny reservation. CZ, EE, IT, NL, SI and UK thought this article was superfluous.

112 COM said that consumer organisations and data protection organisations enhance fundamental rights so it was important that they could lodge complaints.

113 IT scrutiny reservation.

114 DE parliamentary reservation; BE, EE reservation and IT scrutiny reservation. EE, supported by FI and 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.

115 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.

116 COM reservation on limitation to competent supervisory authority.

117 This paragraph was moved from Article 73(3). BE, EE, FR reservation. BG, DE, DK, IT, LU, NL, PT and UK scrutiny reservation. UK in particularly 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 thought that paragraph 1 was sufficient. For DK, PL and SE it was not acceptable that an organisation etc. had an independent right to lodge a complaint.

2. (…)

3. (…)

4. (…)

5. (…)[118]

Article 76a

Suspension of proceedings[119]

1. Where a competent court of a Member State has reasonable grounds to believe that proceedings concerning the same processing activities are pending in a court in another Member State, it shall[120] contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings involving the same processing activities are pending in a court in another Member State, any competent court other than the court first seized may suspend[121] its proceedings.

---

118 COM scrutiny reservation on deletion of paragraphs 3 to 5. FR reservation on the deletion of paragraphs 3 to 4.

119 AT, BE, DK, EE, ES, FI, FR, IT, NL, PL, PT, SE and SI 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.

120 LU supported by EL, suggested to replace "shall" with "may".

121 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.

2a. Where these proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.[122]

Article 76b

Actions before the Court of Justice of the European Union against decisions by the European Data Protection Board

1. Actions may be brought before the Court of Justice of the European Union in accordance with Article 263 TFEU, in order for it to review the legality of decisions taken by the European Data Protection Board pursuant to Article 58a. Such actions may be brought before the Court of Justice of the European Union by supervisory authorities, Member States and the Union institutions as well as by natural or legal persons to whom decisions taken by the European Data Protection Board have been notified or to whom such decisions are of direct and individual concern, including data subjects who have lodged a complaint in accordance with Article 73.
2. The expiration of the time-period provided for in the sixth subparagraph of Article 263 TFEU and the Rules of Procedure of the General Court shall not bar the persons referred to in paragraph 1 from calling in question the lawfulness of any decision taken by the European Data Protection Board before the national courts in accordance with Article 74 or 75 and those national courts from requesting the Court of Justice of the European Union a preliminary ruling concerning the validity of any decision taken by the European Data Protection Board in accordance with Article 267 TFEU.

[122] Based on Article 28 of Brussels I Regulation.

3. Where the European Data Protection Board notifies its decision in accordance with Article 58a(6), such a notification shall state the possibility for the persons referred to in paragraph 1 to bring an action for annulment before the General Court of the European Union in accordance with Article 263 TFEU as well as the time-period for such an action in accordance with the sixth subparagraph of Article 263 TFEU and the Rules of Procedure of the General Court. It shall also refer to the additional right conferred on that person pursuant to paragraph 2.
4. In the event that the European Data Protection Board has an obligation to act and fails to take a decision, proceedings for failure to act may be brought before the Court of Justice of the European Union in accordance with Article 265 TFEU.
5. The European Data Protection Board shall be required to take the necessary measures to comply with the judgment of the Court of Justice of the European Union.

Article 77

Right to compensation and liability[123]

1. Any person who has suffered [124]damage[125] as a result of a processing operation which is not in compliance [126] with this Regulation shall have the right to receive compensation from the controller or processor[127] for the damage suffered.[128]

2. [129]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[130] and severally liable for the entire amount of the damage This is without prejudice to recourse claims between controllers and/or processors[131].

---

123 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.

124 DE, HU and SK suggested adding "material or immaterial/moral". NO suggested clarifying this in a recital.

125 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.

126 COM reservation as the current draft (contrary to the initial version and the 195 Directive) no longer embodies the principle of strict liability.

127 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 this is already encompassed in the current draft.

128 SE supported by HU considered that Article 77 was unclear and wanted to know whether both an economic and immaterial damage was covered.

129 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?

130 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.

131 SI reservation: SI thought this paragraph could be deleted and left entirely to national law.

3. The controller or the processor may[132] 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[133].

4. Court proceedings for exercising the right to receive compensation shall be brought before the courts with jurisdiction for compensation claims under national law of the Member State referred to in paragraph 2 of Article 75.

---

132 PL thought this should be turned into a mandatory provision.

133 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.