Comments and proposals
on the Chapter IV of the General Data Protection Regulation

Ahead of the trialogue negotiations later this month, EDRi, Access, Panoptykon Bits of Freedom, FIPR and Privacy International would like provide comments on selected key elements of the Chapter IV on Controller and Processor.

When amendments are proposed **bold** (additions)and ~~strike-through~~ (deletions), these reflect changes from the Commission proposal.

INTRODUCTION

The role of controllers and processors and their accountability is addressed in Chapter IV. It is specially important to take into consideration the idea of using codes of conducts and certification mechanisms. If not carefully supervised by a public authority in the framework of the consistency mechanism, these codes and seals would provide a quick way for corporations to be legally in line with the Regulation without being necessarily compliant in practice. The issues of data protection by design and by default as well as notifications in case of data breaches are further important Article in this Chapter.

Main issues in Chapter IV on controller and processor:

- Codes of conducts and certification mechanisms would only be acceptable provided that:

- privacy seals are issued by or under the authority of a data protection authority and codes of conduct are issued or endorsed by a data protection authority;
- such seals and codes are subject to the consistency mechanism; and, equally importantly
- seals and codes will be legally binding on those to whom they apply, to ensure implementation, enforcement and reddress (see comments to Articles 38 and 42).

  If these safeguards are not in place, codes of conduct and certification mechanisms would become huge loopholes that would undermine the functioning the Regulation.

- The concepts of data protection by design and by default are essential. This means protection needs to be built into any service where personal data is used, and that the default setting must be the most protective for personal data.
- We call for the creation of a public register related to the notified breaches. Keeping such a public register will allow informed public debate about information security.

Article 22 – Responsibility and accountability of the controller

Article 22 takes account of the debate on a "principle of accountability" and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance. We therefore support the Parliament's suggestion of changing the title of this Article to "Responsibility and accountability of the controller".

The Council text includes a provision that would authorise the use of codes of conduct and certification mechanisms as measures demonstrating controllers' compliance with its obligations. This proposal would only be acceptable if certification mechanisms and codes of conduct are issued or endorsed by a supervisory authority to provide the necessary safeguards by the competent public authority and is subject to the consistency mechanism referred to in Article 57.

Nonetheless, the issue of codes and seals must be treated with extreme caution. Experience shows that they are very difficult to enforce, making their use for cross border transfers highly risky. Both of the above-mentioned criteria must be fully respected. Otherwise, all references to these measures as appropriate measures or elements to demonstrate compliance with controller's obligation should be deleted.

With the exception of this proposed modification, our amendment is based on the Commission text and integrates selected improvements suggested by the EDPS.

EDRi's proposal for Article 22

1. **Personal data shall be processed under the responsibility and liability of the controller.** The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. **(a) to (e) deleted**

2a. Adherence to codes of conducts **issued or approved by a supervisory authority** pursuant Article 38 or a ~~certification mechanism~~ **data protection seal** issued or approved by a supervisory authority pursuant to Article 39 may be used as an element to demonstrate compliance with the obligation of the controller.
The issuing or endorsement of codes of conduct and certifications referred to in this Article, shall be subject to the consistency mechanism referred to in Article 57.

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures **taken** referred to in paragraphs 1 and 2**a**. ~~If proportionate, this verification shall be~~

~~carried out~~ by independent internal or external auditors. **The controller shall publish an accountability report at regular intervals.**

3a. In implementing paragraph1, the controller shall take into account the nature, context, scope and purposes of the processing, the risk for the rights and freedoms of individuals and the type of the organisation.

4**. deleted**

Article 23 - Data protection by design and by default

Data protection by design refers to situation where the controller takes a positive approach to protecting privacy, by embedding it into both technology and into their organisational policies. This requires thinking of privacy and data protection from the beginning of the development of a product or service. When such protections are built in from the beginning, they can help to prevent invasions of privacy rights, such as costly data breaches, before they occur and reduce their damage if they do occur - for both citizens and business.

Pivotal to this approach is privacy by default, which means that when a user receives a product or service, privacy settings should be as protective as possible, without the user having to change them. This allows everyone to be guaranteed a high level of protection, facilitating everyone to consciously choose the privacy setting with which they feel most comfortable – rather than the service provider making a guess about what they might prefer. Service providers should support their users in this by providing user-friendly methods to change privacy settings. They should also be transparent about their data processing practices and supply understandable privacy policies.

The concept of "data protection by design" in the Commission proposal needs more specification. Given that in many services such as social networks, the default settings allow wide public sharing of information, the requirements in paragraph 2 should be strengthened. Our amendment will reflect those changes as well as integrating improvements brought by the Parliament proposal to further strengthen privacy by default and design.

EDRi's proposal for Article 23

1. Having regard to the state of the art and the cost of implementation, the controller **and the processor, if any,** shall, both at the time of the determination of the **purposes and** means for processing and at the time of the processing itself, implement appropriate ~~technical and organisational~~ measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject**, in particular with regard to the principles laid out in Article 5. Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures.**

This shall include both:

(a) technical measures relating to the technical design and architecture of the product or service; and

(b) organisational measures which relate to operational policies of the controller.

Where a controller has carried out a data protection impact assessment pursuant to Article

33, the results of this shall be taken into account when developing the measures referred to in points (a) and (b) of this paragraph.

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. **This shall be ensured using technical and/or organisational measures, as appropriate.** In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals **and that data subjects can control the distribution of their personal data**.

3. deleted

4. deleted

Article 24 - Joint controllers

The objective of Article 24 is to clarify the responsibilities of joint controllers as regards their internal relationship and towards the data subject. While the Parliament and Council have brought different improvements to the text, the amendment proposed by the EDPS succeeds in including both in a short and clear text. We therefore recommend following the suggestion of the EDPS for Article 24.

Article 25 - Representatives of controllers not established in the Union

To ensure the uniform application of the Regulation, Article 25 lays down the obligation of controllers not established in the Union to designate a representative in the Union to cover their activities falling under the scope of this Regulation.

Of particular concern under the Commission proposal, Article 25 established an exception permitting businesses with fewer than 250 employees not to have to appoint a representative in the EU. This would make effective enforcement very difficult, if not impossible, causing a major loophole. Smaller companies can hold enormous numbers of records and should therefore appoint a representative in the EU in order to allow for effective enforcement of the Regulation. Without such a representative, a European DPA would have to go to a court in its own country to ask for confirmation of its jurisdiction if the data controller does not comply. This would be extremely time consuming as well as ineffective, as nothing prevents a data controller from going to a court in its own establishment asking for a contradictory ruling. We therefore suggest to base the representation of the number of persons whose data are processed by a controller, as proposed by the Parliament text. This may relate to an employee, a customer, a prospect or a natural person in any other quality. The amount of personal data being processed should be the determining factor, not size of enterprise. Additionally, the exception for controllers established in third countries regarding which a positive adequacy decision has been issued should be removed.

EDRi's proposal for Article 25

1. Where Article 3(2) applies, the controller shall designate in writing a representative in the Union.

2. This obligation shall not apply to:
(a) **deleted**
(b) an enterprise ~~employing fewer than 250 persons~~ **processing personal data relating to fewer than 250 data subjects**; or

(c) a public authority or body;
(d) **deleted**

3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

Article 26 – Processor

The original proposal form the Commission on Article 26 constitutes a very good basis for rules regarding the processor's obligations.

The large number of modifications proposed by the Council does not help clarify the obligations established in this Article and often creates bureaucratic hurdles. We would recommend maintaining a text close to the Commission proposal, as suggested by the EDPS.

Finally, an addition should be made to ensure that the principles of Data protection by design is assessed by the processor.

EDRi's proposal for Article 26

Follow the EDPS recommendation here and add a point (i) to Article 26.2 as follows:

(i) take into account the principle of data protection by design.

Article 27 - Processing under the authority of the controller and processor

Article 27 integrates Article 16 of the Directive 95/46/EC establishing the rules regarding the processing of data by a person acting under the authority of the controller or processor.

While the Council deleted this Article, as it establishes new rules under Article 26, we recommend keeping Article 27 as proposed by the Commission and Parliament for clarity.

Article 28 - Documentation

Article 28 describes the obligation for controllers and processors to maintain documentation of the processing operations under their responsibility.

The Commission and Council establish an exception to this for companies employing fewer than 250 persons. The size of the controller is not the appropriate criterion to trigger an exception, as small controllers can process personal data of large numbers of data subjects. While the Parliament suggests deleting this provision, an alternative solution would therefore be to use the number of data subjects as the threshold criterion. In line with the EDPS 2012 Opinion, the exceptions in paragraph (4) might as well be removed in total, as proposed by the Parliament.

EDRi's proposal **for Article 28**

1. Each controller and processor and, if any, the controller's representative, shall maintain **regularly updated** documentation of all processing operations under its responsibility.

2. The documentation shall contain at least the following information:

(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
(b) the name and contact details of the data protection officer, if any;
(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
(d) a description of categories of data subjects and of the categories of personal data relating to them;
(e) the recipients ~~or categories of recipients~~ of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;
(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;
(g) a general indication of the time limits for erasure of the different categories of data;
(h) the description of the mechanisms referred to in Article 22(3).

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

4. deleted

5. deleted

6. deleted

Article 29 - Co - operation with the supervisory authority

We suggest following the Article 29 as in the EDPS Opinion of 27 July 2015.

Article 30 - Security of processing

We suggest following the Article 30 as in the EDPS Opinion of 27 July 2015.

Article 31 – Notification of a personal data breach to the supervisory authority

As the objective of Article 31 is to create an effective notification mechanism to the supervisory authority in case of personal data breach, we welcome the suggestions made the EDPS which includes several provisions from the Commission initial proposal.

We would however, suggest adding an amendment for the supervisory authority to create a public register of notified breaches. Keeping such a public register would allow public debate about information security. While expeditious notification of data breaches is needed, a 24-hour time limit might be difficult to realistically implement, and could potentially undermine the effectiveness of these provisions. Considering that this provision will apply to many different types of controllers, from small companies to large enterprises, one time limit may not be appropriate in all cases. We therefore suggest extending this to 72 hours, in exceptional circumstances.

EDRi's proposal for Article 31

We suggest following the EDPS version and add the following paragraph:

4a. The supervisory authority shall keep a public register of the types of breaches notified.

Article 32 - Communication of a personal data breach to the data subject

Data breach notification requirements can help to expose sloppy security on the part of controllers and ensure that measures for the speedy remedy of those breaches and the establishment of more security measures will be taken.

We do not support the proposal of the Council based on a “risk based approach” with a long list of exceptions that would limit the reporting obligation. The scale of the risk depends on the specific circumstances of the data subject. For some people, a breach of their postcode would be a high risk (for example, victims of stalking) for some, while for others that breach would be less important. Therefore, our amendment is based on the Commission text, integrates improvements proposed by the Parliament and is in line with recommendations made by the EDPS.

EDRi's proposal for Article 32

1. When the personal data breach is likely to adversely affect the protection of the personal data or the privacy of the data subject **or other fundamental rights**, the controller shall communicate the personal data breach to the data subject without undue delay. 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the

personal data breach and contain at least the information and the recommendations provided for in points (b) **to (e)** of Article 31(3).

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

5. The ~~Commission~~ **European Data Protection Board** shall be **entrusted with the task of issuing guidelines, recommendations and best practices** ~~empowered to adopt delegated acts~~ in accordance with Article ~~86~~ **66** for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely **or seriously** affect the personal data referred to in paragraph 1.

6. deleted

Article 33 - Data protection impact assessment

EDRi is pleased that the Regulation includes a provision on mandatory data protection impact assessment.

In the interest of clarity, our proposed amendment, based on the Commission proposal, demands a data protection impact assessment for all profiling measures.

In line with the EDPS opinion and the Council proposal, we advocate removing the limitation to processing “on a large scale” in paragraph 2 (b),(c) and (d).

Following the proposal from the Parliament, we recommend deleting the exemption in paragraph (5). The modification proposed by the Council to this paragraph leave too much discretion to the Members States and would not benefit the overall objective of harmonisation.

EDRi's proposal for Article 33

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller’s behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The following processing operations in particular present specific risks referred to in paragraph 1:

(a) any processing operation of the kind referred to in Article 20(1) of this Regulation; ~~a~~

~~systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;~~

(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals ~~on a large scale~~;
(c) monitoring publicly accessible areas, especially when using optic-electronic devices ~~(video surveillance) on a large scale~~;

(d) personal data in ~~large scale~~ filing systems on children, genetic data or biometric data;
(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, **including in particular the risk of discrimination being embedded in or reinforced by the operation,** the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned**, covering all stages of the processing. This assessment shall be kept up-to-date.**

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

5. deleted

6. deleted

7. deleted

Article 33a – Data protection compliance review

EDRi welcomes this new Article introduced by the Parliament strengthening the functioning of the data protection impact assessment by requesting a periodic compliance review. We therefore suggest adding this Article as proposed by the European Parliament.

Article 34 - Prior authorisation and prior consultation

EDRi suggests an amendment improving safeguards relating to third-country transfers, profiling, processing of health data, and processing for research purposes, in line with proposals from the Parliament.

Seals and code of conduct can also require certain technical measures, which will be normally laid down in technical specifications. The EU normally requires the quality of "common technical specifications" for such technical specifications to be taken into accountfor regulatory compliance.

The suggested new paragraph 3b would serve to create certainty for actors willing to invest in complex technical developments that would help in achieving the goals of data protection. Such developtmentscould be a technical specification that accompanies a certain seal or code of conduct, but also a technical specification that creates a certain seal.

EDRi's proposal for Article 34

1. **deleted**

2. The controller or processor acting on the controller's behalf shall consult the **data protection officer, or in case a data protection officer has not been appointed, the** supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks**, including in particular the risk that the operations may have a discriminatory impact**; or

(b) the **data protection officer or** supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

3a. The supervisory authority shall seek the views of representatives of the data subjects and of the Data Protection Board on the intended processing,

3. Where the **competent** supervisory authority **determmines** ~~is of the opinion~~ that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

3b. The data protection board may determine that compliance with a common technical specification creates the presumption of compliance with the the present regulation or parts thereof. The data protection board may request the European Commission to issue a delegated act in accordance with Article 86 to make this assessment binding upon all data protection authorities.

4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

5. deleted

6. deleted

7. deleted

8. deleted

9. deleted

Article 35 - Designation of the data protection officer

EDRi suggests using the amendment proposed in the EDPS opinion, which provides clear rules for the designation of the data protection officer.

Article 36 - Position of the data protection officer

EDRi does not have specific comments on this Article, which is broadly similar to the versions proposed by the Commission, Parliament and Council. As the EDPS suggests a clear provision gathering good elements from the three institutions, we recommend following the EDPS proposal.

Article 37 - Tasks of the data protection officer

Article 37 establishes the core tasks of the data protection officer. As the EDPS suggests a clear provision, we recommend following the EDPS proposal.

Article 38 – Codes of conduct

Article 38 concerns codes of conduct, building on the concept of Article 27(1) of the Directive 95/46/EC. It aims at clarifying the content of the codes, setting procedures for their submission and approval, and providing for the decision on the general validity of codes of conduct.

Codes of conduct can be helpful in providing clarity on how particular sectors are implementing the Regulation, and contributing to uniform application of the law across the Member States; they can only be considered as part of a mechanism guaranteeing appropriate safeguard for the transfer of data to third countries, if they have been approved by a data protection authority, subject to the consistency mechanism and, equally importantly, they're subject to legally binding instrument to ensure implementation, enforcement and redress (see also comments to Article 42). The Council has made a proposal that opens the gates to a massive Trojan horse rule for the transfer of data. Under the proposed provision, codes of conduct could be used to authorise the transfer of data towards, and the onwards transfer of data to, countries where privacy enforcement is weak. Furthermore, the envisaged systems of monitoring and oversight are delegated to private bodies. Public authorities and bodies would also be authorised to transfer personal information at will to public bodies outside the EU without any reference to data protection authorities or need for cooperation across the EU. This situation must be prevented. Finally, our proposed amendment partly includes proposal from new Article 38a on the monitoring of approved codes of conduct, which was created by the Council. Therefore we suggest not having Article 38a as a different Article in the Regulation.

Our proposal for this Article *must* be read together with our proposal on Article 42.

EDRi's proposal for Article 38

1. The Member States, the supervisory authorities, **the European Data Protection Board** and the

Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

(a) fair and transparent data processing;

(aa) guarantee the observance of the principles of personal data processing as established in Article 5;

(b) the collection of data;

(c) the information of the public and of data subjects;

(ca) guarantee data subject rights as established in Chapter III.;

(d) requests of data subjects in exercise of their rights;

(e) information and protection of children;

(f) transfer of data to third countries or international organisations;

(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them ~~to an opinion of~~ **for approval by** the supervisory authority in that Member State. The supervisory authority **may approve a** code of conduct or **an** amendment if **it** is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the **European Data Protection Board for an opinion.**

4. ~~**After consultation with the European Data Protection Board**~~**, If the opinion of the Board is positive,** the Commission may adopt ~~implementing~~ **delegated** acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to the Board ~~it~~ pursuant to paragraph 3 have general validity within the Union. Those ~~implementing~~ **delegated** acts shall be adopted in accordance with the examination procedure set out in Article 8**6**~~7(2)~~.

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

Article 39 - Certification

The possibility of introducing certification mechanism created by this Regulation could provide valuable information to data subject when using a service or a product and could be recognised as a mechanism guaranteeing appropriate safeguards for the transfer of data to third countries under strict criteria.

However, as for the code of conduct, it is important to avoid the certification mechanism being useable as a Trojan horse for the transfer of data to third countries with non-existent or weak protection for data subject's personal information. This would be possible under the proposal made by the Council and would leave the data subject's with little or no control over their personal information. In many cases, the data subject would even not be aware of the transfer.

If certification mechanisms are not issued or endorsed by a supervisory authority and subject to the consistency mechanism, they then must not be used for transfers.

Our proposal for this Article *must* be read together with our proposal on Article 42.

EDRi's proposal for Article 39

1. The Member States, **the European Data Protection Board** and the Commission shall encourage~~, in particular~~ at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

1a. In addition to adherence by controller and processor subject to the Regulation, certification mechanisms and data protection seals and marks issued or endorsed pursuant paragraph 1b may provide appropriate safeguards within the framework of personal data transfers to third countries or international organisation under the terms referred to in Article 42.

1b. Certification mechanisms and data protection seals and marks shall be issued or endorsed by a supervisory authority and shall be subject to the consistency mechanism referred to in Article 57. The supervisory authority shall monitor compliance with the code of conduct.

2. The Commission shall be empowered to adopt**, after requesting an opinion of the European Data Protection Board,** delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.

3. The Commission, **with the European Data Protection Board**, may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those ~~implementing~~ **delegated** acts shall be adopted in accordance with the examination procedure set out in Article 8**6**~~7(2)~~.

Relation of Articles 38 and 39 with Article 42 – Transfers by way of appropriate safeguards

As stated in our comments on the Chapter V of this Regulation, certification mechanisms and codes of conduct can be allowed to provide "appropriate safeguards" for transfers only if they are issued or at the very least endorsed by a supervisory authority and they are subject to the consistency mechanism, and backed by a legally binding instrument.

Nonetheless, the question of codes and seals must be treated with extreme caution. Experience and years of evidence shows that they are very difficult to enforce, making their use for cross-border transfers highly risky if a binding legal agreement or instrument is not in place to ensure that enforcement can actually effectively be carried out in practice and redress is actually available. Experience *proves* that self-regulation alone doesn't work in this context. The above-mentioned criteria must be fully respected. Otherwise, all references to these measures as appropriate safeguards for third country transfer should be deleted.

We recommend that appropriate safeguards shall:

a) guarantee the observance of the principles of personal data processing as established in Article 5;
b) guarantee data subject rights as established in Chapter III.

EDRi's proposal for Article 42

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data contained in a legally binding instrument.

2. The appropriate safeguards referred to in paragraph 1 shall be provided for by:

(a) binding corporate rules approved by a supervisory authority in accordance with Article 43; or
(aa) a code of conduct or certification issued or endorsed by a supervisory authority in accordance with Article 38 and 39; or.
(b) standard data protection clauses adopted by the Commission. Those ~~implementing acts~~ shall be adopted in accordance with the examination procedure referred to in Article 87(2);
(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 ~~when declared generally valid by the Commission pursuant to point (b) of Article 62(1)~~; or
(d) contractual clauses between the controller or processor and the recipient of the data approved by a supervisory authority in accordance with paragraph 4.

2a. The issuing or endorsement of codes of conduct and certifications referred to in paragraph (2) at (aa), the approvals of binding corporate clauses and contractual clauses referred to in paragraph (2) at (a) and (e), and the adoption of standard clauses referred to in paragraph (2) at (d), when related to processing involving a data transfer or transfers, shall be subject to the consistency mechanism referred to in Article 57.

3. deleted

4. ~~Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article t~~ **T**he controller or processor shall obtain prior authorization of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority **for transfers according to this Article**. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5. ~~Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.~~ Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.