



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

Ahead of the trialogue negotiations in September, EDRi, Access, Panoptikon, Bits of Freedom, FIPR and Privacy International would like provide comments on selected key elements of the Chapter III on Rights of the data subject.

When amendments are proposed **bold** (additions) and ~~strike-through~~ (deletions) reflect changes in comparison with the Commission's initial proposal.

INTRODUCTION

In order to have a strong Data Protection framework, citizens (“data subjects”) or groups of citizens need to have recognised rights that empower them to exercise their data protection and privacy rights. For example, individuals should be able to assert their rights faced with incorrect or out of date credit blacklisting.

It is also important that governments not have the right to arbitrarily or non-transparently produce profiles of citizens. Profiling is a process whereby assumptions are made about individuals based on automated processing of data which has been collected about them. This type of profiling is most commonly used for certain business purposes (for targeted advertising or credit rating, in particular). Profiling tends to reinforce societal stereotypes and has a built-in acceptance of errors – the profile will guess who is a potential terrorist or a bad insurance risk. “Big data” vastly decreases transparency, while increasing the risks associated with automated decision-making. Both the collection and processing of data for this purpose, as well as the “outputs” need to be rigorously regulated in order to ensure that the legal framework is adequate for current and future challenges.

Main issues in Chapter II on Data subject rights:

- General rules that guarantee data subjects' control over their personal information in Article 10a.
- We call for the re-introduction of Article 11, which contained a requirement for “concise, transparent, clear and easily accessible policies” about how personal information is being used.

- The controller should be required to establish procedures and mechanisms to facilitate the exercise of the rights pursuant to Articles 13 to 20, as proposed by the European Parliament and EDPS.
- Until a clear definition and further guidance on the meaning of “disproportionate” means in this context, we suggest removing this exception in Article 13.
- Information should be given to data subjects in writing and, where possible, in electronic form. Information rights must logically also cover profiling measures.
- We propose adding a measure to strengthen the ability of the data subject to exercise his or her right to erasure in case where the controller no longer exists and cannot be identified.

Article 10a – General principles for data subject rights

The proposed Article 10a added by the European Parliament provides added clarity on the objectives of this chapter and lays down general rules for data subject rights that would ensure data subjects' control over their personal information. **We therefore support the addition this article.**

Article 11 – Transparent information and communication

In order to have a strong Data Protection framework, data subjects need to have certain key rights that uphold their fundamental right to privacy and data protection. A cornerstone of the enjoyment and exercise of those rights is the provision of clear and transparent information on the processing of their personal information by the controller. This right is defined by Article 11 of the Commission proposal and Parliament text.

As the Council's proposal moved part of this article into Article 12, the obligation for controllers to provide such information is now vague and its scope is reduced. This could make it more difficult for people to effectively exercise their rights under this Regulation, as they would not necessarily be aware of the processing, which would remove control over their personal information. Such a situation could also be problematic for controllers, as the processing of inaccurate or outdated data may be more likely to take place if data subjects are unaware of their rights to access and rectification.

We strongly recommends re-introducing Article 11, as it had concrete obligations on how people, especially children, need to be informed in a “concise, transparent, clear and easily accessible policies” about how personal information is being used – **in line with the Parliament's suggestion.**

Article 12 - Procedures and mechanisms for exercising the rights of the data subject

Article 12 of the Regulation aims at establishing a clear obligation for the controller to provide procedures and mechanisms for exercising the data subject's rights, including laying down time and format requirements for responses to the data subject's request, and the justification of refusals to carry out a request, if applicable.

To fully protect those rights and ensure a prompt response from the controller, we recommend taking Article 12 as proposed by the **Commission as a basis**, and bring in improvements proposed by the EU Parliament as well as **suggestions made by the EDPS:**

- The controller shall establish procedures and mechanisms to facilitate the exercise of the rights pursuant to Articles 13 to 20 as proposed by the European Parliament and EDPS.
- Following the Commission proposal, the controller shall notify the data subject without undue delay, at the latest within a month, of receipt of the request. Such period may be extended for a further month, if needed due to the complexity of the request and the number of the requests. The controller has to notify and justify this delay to all relevant data subjects. We see no clear justification for moving away from the Commission's initial suggestions – if data are being processed for business reasons, it should be reasonable to assume that they will normally be readily available for the processor and therefore available to answer a data subject's request.
- Information will be given to data subjects in writing and, where possible, in electronic form, if the data subject's request was submitted electronically, as proposed by the Commission and Parliament. We oppose the Council's suggestion to allow the information to be given only orally.
- If the controller does not take action at the request of the data subject, the controller shall inform the data subject of the reasons for the refusal or inaction and on the possibilities of lodging a complaint to the supervisory authority and seeking judicial remedy as proposed by the Commission and Parliament texts.

Finally, the possibility to permit the controller from fulfilling its obligations under this Regulation, and thus restricting data subject's rights, by circumventing Article 10 and 10.2 as proposed in the Council text must be avoided.

EDRI's proposal for Article 12

1. The controller shall establish procedures ~~for providing the information referred to in Article 14 and for the~~ **and mechanisms to facilitate** the exercise of the rights of the data subjects referred to in Articles 13 to 20. ~~The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.~~

2. The controller shall ~~shall inform~~ **provide the information referred to in Articles 13 to 15 and information on action taken on a request under Articles 16 to 20** to the data subject without undue delay and, at the latest within one month of receipt of the request ~~whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information.~~

This period may be ~~prolonged for~~ **extended when necessary for up to** a further month, if ~~several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller~~ **taking into account the complexity of the request and the number of the requests. Where the extended period applies, all relevant data subjects shall be informed as soon as possible.**

Where the data subject makes the request in electronic form, the information shall be provided in electronic form where possible, unless otherwise requested by the data subject. **Otherwise**, the information shall be given in writing.

2a. Before disclosing any information in response to an access request from a data subject under Article 15 of this Regulation, and before responding to a request for the exercise by a data subject of any of the other rights under Articles 13 to 19 of this Regulation, the controller shall ensure that the identity of the data subjects is reliably checked and authenticated. The provision by a controller of information on a data subject to another person pretending to be that data subject and making such an access request shall constitute an unauthorised disclosure within the meaning of Article 30(2) and a personal data breach within the meaning of Article 4(9) of this Regulation. Article 77 shall apply to any action

taken by the controller in response to any such request or exercise of a right by a person falsely claiming to be the data subject.

3. If the controller ~~refuses to~~ **does not** take action ~~on~~ **at** the request of the data subject, the controller shall inform the data subject of the reasons for the refusal **or inaction** and on the possibilities of lodging a complaint to the supervisory authority and seeking judicial remedy.

4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

5. *deleted*

6. *deleted*

Article 13 - Notification requirement in the event of rectification and erasure

Article 13, based on Article 12(c) of Directive 95/46/EC, provides rights in relation to recipients regarding decisions taken by data subjects to modify or erase their information. This notification mechanism not only ensures that data subjects' decision will be fully implemented, but also guarantees up to date information for all recipients.

While the Council proposes removing this article, the Commission and Parliament's proposals included an exception for the controller to notify all recipients if it involved a “disproportionate effort”. Until a clear definition and further guidance on the meaning of “disproportionate” means in this context, we suggest removing this exception.

EDRI's proposal for Article 13

The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible ~~or involves a disproportionate effort~~. **The controller shall inform the data subject about those recipients if the data subject requests this.**

Article 13a – Standardised information policies

The purpose of this new article added by the European Parliament is the creation of so-called privacy icons that aim to help data subjects to better and more easily understand how data controllers and processors are processing their personal information.

Similar EU-funded initiatives such as the [Platform for Privacy Preferences \(P3P\) Project](#) have put forward similar methods to enable websites to display accessible information regarding their privacy practices.

While the EU Parliament recommended the creation of six icons in a three columns table, we recommend the removal of the proposed first three icons which refer to the principles of purpose limitation, data minimisation and rules on further processing. As compliance with those principles is obligatory, the creation of an icon could lead to confusion. A compliant company that does not provide such an icon could be wrongly considered being engaged in practices that infringe the EU

data protection framework, while the display of such icon could be wrongly understood by data subjects as if particular privacy-friendly measures beyond mere compliance are taking place. We propose restricting icons to those which would reflect whether a company is taking additional privacy-friendly measures.

Uniform standards shall be designed and approved by the European Commission, in close cooperation with the European Data Protection Board. Finally, to prevent possible abuse and misinformation to data subjects, supervisory authorities should be empowered to verify the information displayed on the icons and data subjects should have access to remedy mechanisms in case of false claims from the controller.

EDRi proposal for Article 13a and Annex 1

(**bold** and ~~strike-through~~ show differences with Parliament text)

Article 13a

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with the following particulars:

(a) ~~deleted~~

(b) ~~deleted~~

(c) ~~deleted~~

(d) whether personal data are disseminated to commercial third parties;

(e) whether personal data are sold or rented out;

(f) whether personal data are retained **or communicated** in **un**encrypted form.

2. The particulars referred to in paragraph 1 shall be presented pursuant to Annex 1 in an aligned tabular format, using text and symbols, in the following three columns:

(a) the first column depicts graphical forms symbolising those particulars;

(b) the second column contains essential information describing those particulars;

(c) the third column depicts graphical forms indicating whether a specific particular is met.

3. The information referred to in paragraphs 1 and 2 shall be presented in an easily visible and clearly legible way and shall appear in a language easily understood by the data subjects of the Member States to whom the information is provided. Where the particulars are presented electronically, they shall be machine readable.

4. Additional particulars shall not be provided. Detailed explanations or further remarks regarding the particulars referred to in paragraph 1 may be provided together with the other information requirements pursuant to Article 14.

Article 14 – Information to the data subject

The objective of Article 14 is to further specify the controller's information obligations towards the data subject. To that end, we recommend the following modifications to the texts proposed by the Commission, Parliament and Council:

- extend the right to information of data subject to **cover profiling measures**;
- include information related to possible security measures taken to improve the protection of personal data, and;
- addition of a **mandatory standard format** to provide information to ensure clarity and uniformity and criteria for the development of those standards.

The Council proposes two separate limited articles on information to be given to the data subject, when the data has been collected from him/her directly or when it was obtained by a third party. We recommend keeping the rules under one single article covering both situations as data subjects' right to information should remain consistent, independent of the means by which the controller acquired his/her data.

EDRi proposal on Article 14

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;

(b) **all the specific purposes of the processing for which the personal data are intended as well as information regarding the actual processing of personal data**, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller, **as well as the reasons why the controller thinks that these legitimate interests overrides the interests or fundamental rights and freedoms of the data subject**, where the processing is based on point (f) of Article 6(1);

(c) the period for which the personal data will be stored;

(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;

(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

(f) the recipients or, if appropriate, categories of recipients, of the personal data;

(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;

(ga) where the controller processes personal data as described in Article 20(1), information about the existence of processing for a measure of the kind referred to in Article 20(1) and the intended or possible effects of such processing on the data subject;

(gb) information regarding specific security measures taken to protect personal data;

(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.

3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.

4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:

(a) at the time when the personal data are obtained from the data subject; or

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are common technical specifications that specify technologies helping the user to understand the extent and impact of the data collection. Those technologies are then deemed to fulfill the requirements in Article 13a and 14 of this Regulation. first disclosed.

5. Paragraphs 1 to 4 shall not apply, where:

(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or

(b) the data are not collected from the data subject and the provision of such information proves impossible ~~or would involve a disproportionate effort~~; or

(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law, **if and to the extent that the law in question allows the body collecting the data not to inform the data subject, for so long only as this is necessary for the processing in question**; or

(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.

6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for

8. of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in

point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.

8. The Commission shall lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary, as well as the needs of the relevant stakeholders, including the possible use of layered notices. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 15 – Right to access and to obtain data for the data subject

Article 15 establishes the right for the data subject to obtain information from the controller regarding the processing of his/her personal information.

Pursuant to this right, the data subject shall be able to make a request regarding his/her personal data at any time, in accordance with Article 12.4. The original proposal from the Commission on this article regarding data subjects' right of access in relation to measures based on profiling should be strengthened following the proposals made by the Council to bring this article in line with provisions from the current Directive 95/46/EC.

Finally, while we do not object in principle of the proposal from the EU Parliament to move the right to data portability within this article, we suggests keeping it within Article 18.

EDRI's proposal on Article 15

1. **Subject to Article 12(2a) and (4)**, the data subject shall have the right to obtain from the controller at any time, on request, **in clear and plain language**, confirmation as to whether or not personal data relating to the data subject are being processed, **and as to whether the controller takes measures or intends to take measures in respect of the data subject that are based on profiles as referred to in Article 20(1)**. This shall also apply to data which only permit singling out **a person without identifying that person by name**, where the data subject can verifiably authenticate him/herself. Where such personal data are being processed, **and/or such measures are taken or planned**, the controller shall provide access to the data and the following information:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipients to whom the personal data are to be, **may be** or have been disclosed, in particular to including all recipients in third countries;
- (d) the period for which the personal data will be stored;
- (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;
- (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
- (g) communication of the personal data undergoing processing and of any available information as to their source;
- (h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.

(i) in the case of measures based on automated processing including profiling referred to in Article 20, meaningful information concerning the logic involved in the profiling;
(j) where applicable, in what manner and for what specific purposes the data will be processed for statistical purposes or in pseudonymised form and how it will be ensured that data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information, and more generally how re-identification of the data subjects is to be prevented.

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing, **including profiles generated through automatic means or when this is not possible, the categories into which data subjects are placed on the basis of these profiles.** Where the data subject makes the request in electronic form, the information shall be provided in electronic form unless otherwise requested by the data subject.

3. deleted

4. deleted

Article 16 – Right to rectification

Article 16 further develops the right to rectification created under the Directive 94/46/EC, and helps ensure data subjects' control over their personal information.

The text proposed by the three institutions are relatively straightforward, we therefore propose a combination of good elements from those three. We also suggest adding a second provision, recommended by the European Data Protection Supervisor, to ensure that processing of inaccurate data will be prevented.

EDRI's proposal on Article 16

The data subject shall have the right to obtain from the controller **without undue delay** the rectification of personal data relating to ~~them~~ **him or her** which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by ~~way means~~ **means of supplementing providing** a corrective statement, **and the right to add a supplementing statement to data that are contested by the data subject.**

Article 17 – Right to erasure

Article 17 builds on the Article 12 of Directive 95/46 on the right to erasure, extensively and often inaccurately discussed in the context of the *Google Spain* ruling of 2014.

While the Commission and Council suggest to entitle this **right “to erasure and to be forgotten”**, this formulation is misleading and could lead to confusion with concepts from press law, as we have seen in the aftermath of the so-called *Google Spain* ruling. Since the essence of this right is the **right to erasure**, the title should be changed accordingly, as proposed by the European Parliament.

While the proposals from the Parliament and Council are relatively similar, the Council decision to break the Article into three – Article 17, 17a and 17b – does not provide greater clarity. All elements should therefore remain into a single article.

Regarding the measures proposed in this article, under paragraph 2, the Commission and Parliament request controllers to contact all entities processing data that has been published to take all reasonable steps in order to erase the data. The Council also includes this notification obligation in a new Article 17b. The scope of this obligation is unclear and seems to duplicate the obligation from Article 13 requesting that controller communicate any rectification or erasure to all recipients to whom personal data have been disclosed. For sake of clarity, we therefore recommend removing it.

Finally, we propose adding a measure to strengthen the ability of the data subject to exercise his or her right to erasure in case where the controller no longer exists and cannot be identified.

EDRI's proposal for Article 17

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to ~~them~~ **him or her without undue delay** and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) ~~or when the storage period consented to has expired~~, and there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;

(d) the processing of the data does not comply with this Regulation for other reasons have been unfairly or unlawfully processed.

2. deleted

3. The controller, **and, where applicable, the third party**, shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

(a) for exercising the right of freedom of expression ~~in accordance~~ **provided all the requirements and safeguards of with Article 80 are fully complied with;**

(b) for reasons of public interest in the area of public health ~~in accordance~~ **provided all the requirements and safeguards of with Article 81 are fully complied with;**

(c) for historical, statistical and scientific research purposes ~~in accordance~~ **provided all the requirements and safeguards of with Article 83 are fully complied with;**

(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; such Union or Member State laws shall meet an objective of essential public interest, fully respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;

(e) in the cases referred to in paragraph 4.

3.1 When the controller no longer exists or cannot be identified or contacted, the data subject has the right to obtain the erasure of personal data relating to him or her from third parties that process that personal data, where the same grounds apply as in Article 17(1).

4. Instead of erasure, the controller **or processor** shall restrict processing of personal data, **in such a way that it is not subject to the normal data access and processing operations of the controller and can not be changed anymore**, where:

(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;

(b) the controller no longer needs the personal data for the accomplishment of its **original** task but they ~~have to be maintained for purposes of proof~~ **are required to retain the data by the law or the data subject for the establishment, exercise or defense of legal claims; in those cases, the controller may only use the data in relation to those claims.**

(c) the processing is **unfair or** unlawful and the data subject opposes their erasure and requests the restriction of their use instead;

(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the processing that the data concerned must be restricted;

(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Articles **15 and 18**.

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.

7. The controller and processor shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

8. Where the erasure is carried out, the controller shall not otherwise process such personal data.

9. The Commission shall be empowered, **after requesting an opinion from the European Data Protection Board**, to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:

(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;

(b) the conditions for deleting ~~links, copies or replications~~ of personal data from publicly available communication services as referred to in paragraph 2;

(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.

Article 18 – Right to data portability

Data portability is a key element to strengthen the rights of the data subject, as well as to ensure healthy competition, as it would prevent consumers from being locked into a service, as it the case now for most current online services

While the proposal from the Council appears to limit this right, the European Parliament has decided to move the core element of this right into Article 15. We consider the latter to be an unsatisfactory compromise solution, since the purpose of the two articles is different. Our suggestion aims at improving the original proposal from the European Commission, which created a dedicated right to data portability in Article 18.

Our proposal reflects the following changes:

- **Full applicability of the right to data portability** can only be ensured if it is extended to cases beyond processing based on contract or consent. Similarly, controllers should not have the possibility to refuse to make the data available by claiming that the format used is not “commonly used”.
- It should be clarified that this right is without prejudice to the obligation to delete data when they are no longer needed.

EDRI's proposal for Article 18

1. The data subject shall have the right, where personal data are processed by electronic means ~~and in a structured and commonly used format~~, to obtain from the controller a copy of data undergoing processing in an electronic, **interoperable**, ~~and structured~~ format which ~~is commonly used and~~ allows for further use by the data subject.
2. Where the data subject has provided the personal data ~~and the processing is based on consent or on a contract~~, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.
 - 2a. **This right is without prejudice to the obligation to delete data when they are no longer necessary under Article 5.**
3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 19 – Right to object

The right to object is essential for restoring the balance between the interests of the data controller and data subject.

Following the proposal made by the Parliament, the right to object without having to demonstrate compelling legitimate grounds should be extended to all processing based on Article 6(1)(f).

EDRI's proposal for the right to object

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d) and (e) ~~and (f)~~ of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

2. Where personal data are processed for direct marketing purposes **or where processing is based on Article 6(1)(f)**, the data subject shall have the right to object free of charge to ~~the~~ **such** processing of their personal data ~~for such marketing~~. This right shall be explicitly offered to the data subject in an intelligible manner, **using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child**, and shall be clearly distinguishable from other information.

2a. The controller shall inform the data subject of the action taken in response to an objection under paragraph one within one month, which can be extended to two months in complex cases or cases involving numerous objections. If the data subject does not agree with the action taken by the controller, he or she has the right to take the issue to the competent supervisory authority, who shall issue a binding ruling on the action to be taken, subject to such legal appeals as may be provided for by law.

3. Where an objection is upheld ~~pursuant to paragraphs 1 and 2~~, the controller **shall immediately cease the processing in question**.

Article 20 – Profiling

Insofar as the proposal for a Regulation is a response to the challenges of technological development, there is probably no bigger threat to privacy and data protection in the era of “big data” than profiling.

Profiling means collecting and using pieces of information about individuals to make assumptions about them and their future behaviour, using algorithms or any other methods.

With hugely increased data collection and ever-growing computing power, these algorithms are becoming extremely complicated. The algorithms are not designed to be perfect, and the rarer the characteristics they are used to predict, the higher the likelihood of mistakes. In simple terms profiling should never be used in relation to characteristics that increase the error rate beyond reasonable limits, nor to make significant decisions about individuals. Also, profiles and profiling algorithms can be hard or impossible to assess.

Profiling poses a fundamental threat to the most basic principles of the rule of law and the relationship between citizens and government or between customers and businesses in a democratic society. Often, these algorithms qualify as commercial secrets and will not be easily provided or explained to data subjects. However, when natural persons are subject to profiling, they should be entitled to information about the logic used in the measure, as well as an explanation of the final decision if meaningful human intervention has been used. This helps to minimise the lack of transparency, which could undermine trust in data processing and may lead to loss of trust, especially in online services.

There is also a serious risk of unreliable and, in effect, discriminatory profiles being widely used, in matters of real importance to individuals and groups. This is the motivation behind several suggested changes in this Article that aim to improve the protection of data subjects against positive or negative discrimination. In relation to this, the use of sensitive data in generating profiles should also be avoided.

Finally, it should be specified that the general prohibition applies to all kinds of profiling, both online and offline.

EDRI's proposal on Article 20

1. Every natural person shall have the right, **both off-line and online**, not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely **or partly** on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

1a. No judicial or administrative decision shall be based on measures as described in paragraph 1.

1a. In all cases in which such measures are taken or intended to be taken, this right shall be explicitly brought to the attention of the individual concerned and shall be presented in a manner clearly distinguishable from other matters.

2. Subject to the other provisions of this Regulation, **including paragraphs (3) and (4) of this Article, and without prejudice to paragraph (1a)**, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:

(a) ~~is carried out in~~ **necessary for** the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable ~~measures to~~ **safeguards are put in place to protect** the data subject's legitimate interests ~~have been adduced, such as including the right to be provided with meaningful information about the logic used in the profiling, and the right to obtain human intervention, including an explanation of the decision reached after such intervention;~~ or

(b) is expressly authorized by a Union or Member State law which also lays down suitable ~~measures to~~ **safeguards** the data subject's legitimate interests, ~~including the right to be provided with meaningful information about the logic used in the profiling, and the right to obtain human intervention, including an explanation of the decision reached after such intervention, and which protects the data subjects against possible discrimination resulting from measures described in paragraph 1;~~ or

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards, ~~including effective protection against possible discrimination resulting from measures described in paragraph 1.~~

2a. The suitable safeguards referred to in paragraph 2 shall include the right of the data subject to be provided with meaningful information about the logic used in the profiling; the right to put forward the data subject's views and arguments; the right of the data subject to obtain human intervention, including an explanation of the decision reached after such intervention, taking the data subject's views and arguments into account; and effective measures to protect all data subjects against possible discrimination, including regular reviews of the outcomes of the measures to see if they have had any discriminatory effect, intentional or otherwise, on any of the factors listed in Article 21 of the Union Charter of Fundamental Rights.

3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on **include or generate any data that fall under** the special categories of personal data referred to in Article 9.

3a. Profiling that ,whether intentionally or otherwise, has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, or sexual orientation as well as any of the other characteristics and opinions included in Art. 21 of the Charter of Fundamental Rights that can lead to discrimination, or that, whether intentionally or otherwise, result in measures which have such effect, shall be prohibited.

3b. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be used to identify or individualise children.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Articles 14 **and 15** shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject , **as well as the access meaningful information on the logic underpinning the data undergoing processing.**

5. The ~~Commission~~ **European Data Protection Board** shall be empowered to adopt delegated act in accordance with Article 86 for the purpose **entrusted with the task** of further specifying the criteria and conditions for suitable measures to safeguard the data subject's **fundamental rights regarding the provisions of this Article, and his or her** legitimate interests referred to in paragraph 2.

Article 21 - Restrictions

Restrictions of controllers' obligations and data subjects' rights shall be limited and clearly defined.

Core element of our proposal is the removal of Article 20, related to profiling, from the list of possible exception to the rules that could be implemented in Member State law.

Without this change, governments could claim national security or public security reasons to profile citizens. This could basically providing a blank cheque to governments which, under various potentially weak justification, may start to profile people based on their online political activities and prepare, for example, blacklists who do not fit with the profile of "normal" citizens. This would most likely lead to violations of Article 21 of the Charter of Fundamental Rights.

The way Article 21 is drafted, the Regulation will increase the number of exceptions in relation to the 95 Directive. It is specially worrying the exception which allows Member States to introduce additional exceptions based on a “general public interest” objective. This objective, by definition, will have nothing to do with the other exceptions listed in Article 21 (e.g. any general public interest purpose will not be associated with national security; not defence; not public security; not the prevention, investigation, detection or prosecution of criminal offences) and could be used for a vast variety of purposes, becoming a major loophole in the Regulation.

Furthermore, although Article 21 of the Regulation requires any “restriction” to “constitute a necessary and proportionate measure in a democratic society”, this can only be tested after legislation that uses any Article 21 exception has been enacted, and after interference has occurred. In order to prevent abuses, data protection authorities should be given an explicit role that allows them to analyse the proposed legislation which might include any of such restrictions and order a formal judicial analysis before adoption of the measure

The inclusion of Article 20 in the provisions of Article 21 are an unequivocal drop in standards compared with the existing Directive.

For a more comprehensive analysis of this Article, see Chris Pounder's article at: <http://amberhawk.typepad.com/files/detailed-analysis-of-a.21-council-text.pdf>

EDRI's proposal for Article 21

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to ~~20~~ **19** and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

(a) deleted

(b) the prevention, investigation, detection and prosecution of criminal offences;~~(c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;~~

(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(e) deleted

(f) the protection of the data subject or the rights and freedoms of others.

2. In particular, any legislative measure referred to in paragraph 1 **must comply with the principles of necessity and proportionality and** shall contain specific provisions at least as to:

(a) the objectives to be pursued by the processing;

(b) and the determination of the controller;

(c) the specific means of processing;

(d) the categories of persons authorised to process the data;

(e) the procedure to be followed for the processing;

(f) the safeguards against any arbitrary interferences with the rights and freedoms of individuals, as enshrined in the Charter of Fundamental Rights by public authorities;

(fa) the safeguards to prevent abuse or unlawful access or transfer;

(g) the right of data subjects to be informed about the application of any restriction to their data;

3. Legislative measures referred to in paragraph 1 shall not impose obligations on private controllers to retain data additional to those strictly necessary for the original purpose.

4. Legislative measures referred to in paragraph 1 shall be notified to the European Data Protection Board for opinion. If the European Data Protection Board considers that the notified measure does not comply with the requirements of paragraph 2, it shall inform the Commission. The Commission shall then consider launching the procedure established under Article 258 of the Treaty on the Functioning of the European Union.