Council of the European Union

Brussels, 10 April 2015
(OR. de, en)

7586/1/15
REV 1

LIMITE

DATAPROTECT 40
JAI 197
MI 199
DIGIT 9
DAPIX 48
FREMP 62
COMIX 144
CODEC 431

Interinstitutional File:
2012/0011 (COD)

NOTE

From:	CZ, DE, IE, ES, FR, HR, NL, AT, PL, PT, FI and UK delegations
To:	Working Group on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	7526/15 DATAPROTECT 39 JAI 196 MI 190 DIGIT 8 DAPIX 47 FREMP 60 COMIX 140 CODEC 415 7084/15 DATAPROTECT 31 JAI 169 MI 159 DRS 23 DAPIX 39 FREMP 50 COMIX 114 CODEC 336
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) - Chapters III and VIII

Delegations find in Annex comments from CZ, DE, IE, ES, FR, HR, NL, AT, PL, PT, FI and UK delegations on General Data Protection Regulation - Chapters III and VIII.

This REV 1 incorporates ADD 1 + ADD 2 to the initial version of this document.

TABLE OF CONTENT

CZECH REPUBLIC

Proposals on Chapter III and Chapter VIII

Recital 53a

CZ is doubtful whether to keep recital 53a, which is dealing with single judgment. If so, however, ***Recital 53a*** *should be amended to avoid overreach of the second sentence:*

Inasmuch as the removal of links from the list of internet search results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst **in such cases** the data subject's rights protected by those articles should override, as a general rule, the interest of internet users, that balance may in specific cases depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having access to that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

Recital 54aa

Of the first part, only the first sentence should be kept, as the rest may be interpreted to limit the other rights unduly.

Article 17 – Right to be forgotten and to erasure

Paragraph 1(d) *should read:*

"the data have been unlawfully processed **(manifestly) in abusive manner**".

The goal is to prevent larger injustice in cases when someone in past has not complied fully with all the duties of the Regulation, and now a different controller relies on the data to pursue e.g. his legitimate interests. Erasure of data is the strongest measure available and should be moderated.

Paragraph 2a *should read:*

Where the controller (...) has made the personal data public and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, *shall* ***on request of data subject*** *take (...) reasonable steps, including technical measures, (...) to inform* ~~**known**~~ *controllers* ***to which it intentionally disclosed*** ~~*which are processing*~~ the *data, that a data subject requests them to erase any links to, or copy or replication of that personal data.*

CZ disagrees with this duty, both because it may easily backfire on the data subject (who would not request erasure from certain controllers depending on the context that may change rapidly as evident from paragraph 3) and because it will be difficult to implement and enforce (hence the second amendment, which is at least subject to review of DPA). But our general aim is to give data subject a little more control over the process – there may be reason to ask search engine, but to avoid, at the same time, a social network or news website.

Article 77 – Right to compensation and liability

CZ wishes to propose a compromise system that would both protect the data subject and provide for sufficient flexibility to enterprises which should be free to adopt fitting models of dealing with complaints. Paragraph 2 should be complemented by paragraph 2a, which would read:

However, the first sentence of paragraph 2 shall not apply where a controller or processor clearly and without reservation indicates to the data subject that any such claims should be pursued against such controller or processor.

Article 79 – General conditions for imposing administrative fines

CZ really wishes to preserve a room for manoeuvre for the national DPAs in relation to sanctions imposed on natural persons who are not entrepreneurs. Absolute upper limits are good, but the danger is that EDPB would create single approach that does not respect different (average, median) income levels in Member States. Therefore, we propose to change ***paragraph 2a(m)*** *as follows:*

"any other aggravating or mitigating factor applicable to the circumstances of the case **or to specific situation**."

This should allow any DPA to see imposition of fine on natural person that is not performing its trade, business or profession as specific situation and respect that overall income levels in its Member State are lower or higher than the average.

Alternatively, a recital could be introduced, saying that where the fines are imposed on (natural) persons that are not undertaking, the supervisory authorities may take into account the general level of income in the Member State in considering the appropriate amount of fine.

Article 79b – Penalties

If the intent really is to (a) provide the Member States with opportunity to stipulate criminal sanctions to supplement the administrative ones and ***(b) provide the Member States with opportunity to cover infringements of provisions not listed in Article 79a****, then* ***paragraph 1*** *should read:*

For infringements of the provisions of this Regulation ~~not~~ listed in Article 79a Member States **may** ~~shall~~ lay down the rules on **criminal** penalties applicable to such infringements and shall take all measures necessary to ensure that they are implemented (…). **For infringements of the provisions of this Regulation not listed in Article 79a Member States may ~~shall~~ lay down the rules on penalties applicable to such infringements and shall take all measures necessary to ensure that they are implemented (…).** Such penalties shall be effective, proportionate and dissuasive.

CZ opposes the word "shall", as it is too strict and indeed, does not make good sense in the current text.

GERMANY

Comments and proposals by the German delegation concerning
Recitals 46 - 59 and Articles 11 - 21 of the General Data Protection Regulation
(changes in *bold and italics*)

Recital 48a new

Among other things, Article 21 provides for restrictions by way of legislative measures to the right of access and other rights, for example in the interest of public security or the protection of judicial independence. In formulating these specific exceptions pursuant to Article 21 as needed, the Member States may, in their national law, repeat the wording of the various rights and provisions under the General Data Protection Regulation if the national legislators find this to be necessary in the interest of legal practitioners.

Justification:

- German legislation contains numerous exceptions from data subjects' rights that are necessary because they protect the rights and legitimate interests of third parties and of the data processor as well as public interests (this refers particularly to Sections 19 II through IV; 19a III; 33 II; 34 VII of the Federal Data Protection Act). Very few of these exceptions are contained in the current Council draft. Article 21 provides for the possibility to adopt additional exceptions from data subjects' right, this would mean adopting a national act consisting largely of exceptions. We therefore propose a recital allowing member states to adopt national legislation defining the rights of data subjects in accordance with Chapter III of the General Data Protection Regulation (and insofar repeating the GDPR) and its respective exceptions.

- Because of the direct effect a Regulation has, within the scope of application of a Regulation, member states, as a rule, are not allowed to pass legislation repeating the provisions of that Regulation. However, since the proposed Regulation takes the form of a General Regulation, it provides considerable room for member states to take national legislative measures, e.g. under Article 21. As a result, data protection law will become a complex regulatory system consisting of Union law and member state law turning the application of the law into a challenging task for all parties to which it is addressed. Given this special constellation, it appears appropriate to allow national legislation to repeat certain aspects set out in the Regulation where this is necessary to ensure consistency and understandability for addressees (see ECJ Judgment of 28 March 1985, Commission / Italy (272/83, ECR 1985 p. 1057).

Recital 53a

In as much as the removal of links from the list of internet search results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. ~~***Whilst the data subject's rights protected by those articles should override, as a general rule, the interest of internet users, that balance may in specific cases depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having access to that information, an interest which may vary, in particular, according to the role played by the data subject in public life.***~~

Justification:

This statement, taken from the judgment of the European Court of Justice which ruled that data protection should in general take precedence over the freedom to form opinions and the freedom of information, should not be included in the recitals, because it applies to a specific situation in which the Court of Justice considered the danger of profiling to be particularly pronounced (searches using a person's name). The judgment in question is the first to be handed down on this issue, which will be further clarified in the light of the extensive case-law of the European Court of Human Rights.

Recital 54aa

However the right to be forgotten should be balanced with other fundamental rights. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. This may lead to the result that the personal data has to be maintained for exercising the right of freedom of expression, when required by law or for archiving purposes in the public interest or for historical, statistical and scientific (…) purposes, or, for reasons of public interest in the area of public health or social protection, or for the establishment, exercise or defence of legal claims.

In order to exercise the right to be forgotten, the data subject may address his request to the controller without prior involvement of a public authority, such as a supervisory or judicial authority, without prejudice to the right of the data subject to lodge a complaint or initiate court proceedings against the decision taken by the controller. In these cases it should be the responsibility of the controller to apply the balance between the interest of the data subject and the other interests set out in this Regulation.

Justification:

Clarification.

Article 17c

Dispute Settlements

(1) If a data subject asks a controller operating an Internet search engine (Internet search engine operator) to remove links to web pages from the list of results displayed following a search made on the basis of a data subject's name, published by third parties and containing information relating to that data subject, claiming that the information published violates his privacy, the Internet search engine operator must carefully investigate, whether the requirements of the data subject's right pursuant to Articles 17 or 19 are fulfilled and must hereby respect the rights and interests of any third party affected.

(2) The Internet search engine operator must provide a third party seriously affected an opportunity to submit an opinion on the data subject's request.

(3) The Internet search engine operator must inform the enquiring data subject and the third party seriously affected about the decision and, especially in respect of Article 17 (3), all substantial aspects which were taken into account in the decision-making process.

(4) The Internet search engine operators should set up dispute settlement units in the Member States. The autonomy, independence and plurality of the dispute settlement units and the expertise of their staff must be guaranteed. The dispute settlement units decide about complaints against the Internet search engine operator's decisions pursuant to paragraph 3; these decisions are binding only for the Internet search engine operator. Other remedies of the enquiring data subject and the affected third party, especially the web page operator, in particular according to Chapter VIII, remain unaffected.

Article 20

Profiling

[…]

(4) Decisions referred to in paragraphs 1 and 1a that have the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, genetic or health status, sexual orientation or that result in measures which have such effects, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from such decisions.

(5) The data subject shall have the right to obtain information in a plausible and generally understandable form concerning

(a) the structure and process of the profiling and

(b) the calculation and significance of the probability values including the types of data used with reference to the individual case.

The right to obtain information shall not apply where the request is in conflict with overriding legitimate interests, in particular where trade secrets of the controller would be disclosed.

(6) The controller shall

(a) if necessary to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context in which the personal data are processed, use adequate mathematical or statistical procedures for the profiling,

(b) implement technical and organisational measures appropriate to ensure that factors which result in data inaccuracies are corrected and the risk of errors is minimized,

(c) secure personal data in a way which takes account of the potential threats involved for the interests and rights of the data subject.

Additional comments

I. General comments on Article 77

We believe that the controller should in principle be liable for any damage arising from data processing operations carried out in violation of the GDPR. Processors should be liable only in cases where they have failed to comply with the obligations under the GDPR applicable to processors or where they have acted contrary to lawful instructions from the controller. If necessary, in these cases, the processor and the controller could be held jointly and severally liable.

II. On the basis of this position, we propose the following specific wording for Article 77(1) and (2):

Article 77

Right to compensation and liability

1. Any person who has suffered material and immaterial damage as a result of a processing operation which is not in compliance with this Regulation shall have the right to receive compensation from the controller for the damage suffered. A processor shall be liable for violations of this Regulation only where the processor has acted outside or contrary to lawful instructions of the controller or where obligations of this Regulation specifically directed to processors have been violated.

2. 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, under the conditions laid down in paragraph 1, be jointly and severally liable for the entire amount of the damage. This is without prejudice to recourse claims between controllers and/or processors.

IRELAND

CHAPTER III

Article 17

Paragraph 2a needs to be re-examined in the light of the Google Spain case. In that case the Court noted that the fact that a person might want a search engine to delete a link to personal data in relation to him/her doesn't necessarily mean that the data subject wants the data deleted from the original source. In other words the fact that a data subject wants one controller to delete personal data doesn't automatically mean that he/she wants all controllers to do so. We favour deletion of paragraph 2a for this reason.

Article 18

We support the right to data portability. We are concerned that the reference to the 'right to transmit personal data' has the effect of narrowing the scope of the right to data portability. Our preference would be to replace the word 'transmit' with 'withdraw'.

The right to withdraw personal data should apply only to data provided by the data subject.

This article contains an important data subject right; it should not impose an obligation on controllers to transfer the personal data to another controller.

In order to ensure legal certainty, the text should specify that this right does not apply to controllers processing personal data in the exercise of their public duties (i.e. include text currently located in recital 55).

Article 20

The definition of profiling (article 4(12a)) should cover all types of automated processing (see corresponding text in document 17831/13 of 16 December 2013).

This article should then apply to profiling which produces legal effects or significantly affect a data subject.

The following words should be deleted from paragraph 1: ‘a decision evaluating personal aspects relating to him or her’;

We do not understand how paragraph 1b would apply in cases where a decision is required under Union or Member State law to which the controller is subject (i.e. to situations where paragraph 1a(b) applies). We would therefore suggest that paragraph 1a(b) should be excluded from the scope of paragraph 1b.

Additional comments

CHAPTER III

Article 12

In paragraph 4, we are in favour of retaining "manifestly unfounded".

Article 14

Paragraph 1a

The sub-paragraphs in paragraph 1a need to be re-ordered in a logical sequence, i.e. following the order in Article 6.1(f). This means that

- paragraph (ea), which refers to the 'consent' ground should come first;
- paragraph (g), which refers to a statutory or contractual requirement should come next;
- paragraph (b), which refers to the legitimate interest ground, should follow.
- sub-paragraph (h) will need to be adjusted to take account of the revised wording of Article 20 (see below)

Paragraph 1b

Replace opening words with the following: "Where the controller intends to process the data in accordance with Article 6(4) for a purpose other than the one for which the data were collected ...".

Article 14a

Paragraph 2

The sub-paragraphs need to be re-ordered in the same manner as paragraph 1a of Article 14; sub-paragraph (h) will also need to be adjusted.

Paragraph 3a

See proposed amendment above to paragraph 1b of Article 14.

Article 17

Paragraph 2a

Amend as follows: "... known controllers which are processing the data that the data subject has specifically requested the erasure by such controllers of any links to, or copy or replication of that personal data."

Paragraph 3

Replace subparagraph (a) with the following "for exercising the right to freedom of expression and information referred to in Article 80."

Article 19

Paragraph 1

Replace "on reasoned grounds" with "on compelling legitimate grounds"; restore reference to point (e) of Article 6(1).

Article 20

Paragraph 1

Replace with the following: "The data subject shall have the right not to be subject to a decision based solely on profiling which produces legal effects concerning him or her or significantly affects him or her".

CHAPTER VIII

Article 76

It should be clarified in a recital that this article does not provide for class actions.

Article 77

This article needs to specify who the data subject can seek compensation from.

Article 79

Our understanding of paragraph 1 of this article is that it gives supervisory authorities the power to impose administrative fines but leaves it to the discretion of the supervisory authority concerned as to whether a fine should be imposed in any particular case. In order to avoid uncertainty, "Administrative fines shall,' should be replaced with 'Administrative fines may,".

A reference to article 51a should be added after "Article 51" in paragraph 1.

We support the retention of point (g) of paragraph 2a.

Article 79a

It is essential under our legal system that a controller or processor knows when he/she is, or will be, in breach of the Regulation which may result in the imposition of administrative fine. Legal certainty is essential. However, some of the grounds on which a fine can be imposed are too vague, in particular the following:

(i) "incomplete information" (para. 2(a))
(ii) "timely or in a sufficiently transparent manner" (para. 2(a))
(iii) "not sufficiently determine" (para. 2(e))
(iv) "not sufficiently maintain" (para. 2(f))
(v)Paragraph 3(e);
(vi) "timely" (para. 3(h))

Article 79b

This article should only cover infringements not already covered under article 79a.

It should not provide for the imposition of criminal penalties.

SPAIN

The Spanish position regarding art. 17 is determined by the contents of the Ruling of the European Court of Justice in the "Google case". This Ruling refers to the current legislation, which will be eventually replaced by the draft Regulation, and it might be argued that it has no effects on the current discussions of the draft Regulation, and that the legislative power is not subject to the judiciary. However, the Ruling is crucial because the European Court of Justice not only bases it on secondary law (Directive 95/46/CE), but it also applies and interprets the Charter of Fundamental Rights of the EU (arts. 7 and 8, and partially 11). Due to its privileged position in the architecture of the European legal system, the Charter must determine future legislative action in the European Union. Therefore, the CLEU acted in this case as a "constitutional court", and this decision is relevant for the elaboration of secondary law.

1. All references to the "right to be forgotten", in both recitals and articles, should be deleted

(a) The inclusion of a "right to be forgotten" in art. 17 of the Commission Proposal was perfectly coherent with a situation in which it was unclear whether the activities developed by search engines could be considered as data processing and, if so, whether they act as controllers, processors or mere intermediaries.

(b) The Ruling of the Google case has clarified that:

- Search engines process personal data and they do it as controllers (e.g., paragraphs 35-38, 40 and 83 of the ruling)

- Existing data protection law applies to their activity

- In particular, *"Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages(...)"*

(c) In short, search engines have to apply data protection law like any other controller, without any specificity or particular requirement. The Court does not recognize a new or separate "right to be forgotten", but only the applicability of the classical rights to erasure and to object

(d) Maintaining the present wording ("right to be forgotten and to erasure") is not necessary, in as much as there is nothing such as a right to be forgotten differentiated from the right to erasure and to object. It may also lead to confusion and generate false expectations among data subjects, that might assume that there is a new right whose effects might go beyond the right to erasure.

SECOND.- Art. 17.2a should be deleted if it is intended to address issues related to the activity of search engines.

(a) Art. 17.2a implies a shift in focus with regard to the original art. 17.2 contained in the Commission Proposal. The present version requests controllers that have made data public and that are obliged to delete data upon request of a data subject to inform other controllers of the fact that the data subject requests them to delete links to, or copies of, that information. In the Proposal, the wording was different and the purpose was apparently to establish a "right to be forgotten" independent from the right to erasure.
The present version is not applicable to search engines. They don't "make the personal data public". This data were made public by the editors of the webs whose contents are processed by the search engine and the search engine simply presents them in a different way. Search engines don't process information which has not been made public by web masters.

(b) In any case, and if the paragraph pursues other purposes, references to "links" should also be deleted. If the controller that made the information public erases that that information all links to it will become automatically useless.

THIRD.- Web editors are not entitled to participate in the process of assessment of delisting requests nor affected by its results.

(a) The Ruling draws a clear distinction between the processing of data carried out by the original web editor and the processing carried out by the search engine. They are independent processing operations, with different controllers (e.g., paragraph 86) and different purposes and legal basis. More important, their impact on the rights of citizens is also different. In the case of processing carried out by search engines, the impact is particularly serious by virtue of the universal dissemination and accessibility that search engines offer.

(b) The Court specifically recognizes that while "the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' and thus benefit, by virtue of Article 9 of Directive 95/46, from derogations from the requirements laid down by the directive" that does not appear to be the case with regard to the processing carried out by the operator of a search engine. It may therefore happen that data subjects may successfully exercise their rights against a search engine, but not against the editor of the original web page

(c) According to the Court the rights and interests at stake, apart from those of data subjects, are:

- The legitimate interest (economic interest) of the controller (search engine) does not fully justify the serious interference of the search engine activity on the citizen's right to data protection.

- The legitimate interest of Internet users to access to the information through the search engine, which is related to article 11 of the Charter, with regard to the *"freedom to receive and impart information and ideas without interference by public authority (...)"*.

(d) The ruling establishes that in general, the right to data protection and the right to privacy overrun the Internet user interest of accessing to information. However, that balance may depend, *"in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life."*

(e) The impact of the exercise of erasure and objection rights and of delisting decisions on the freedom of expression, including freedom of information, is, therefore, very limited, for a number of reasons:

-Delisting of links on the results page of a search engine applies only to cases where the search is made using the name of an individual as search terms.

-Information is not deleted from the indexes of the search engine and may be recovered using other search terms different from a personal name (i.e.: topic, date, author, web page,…).

-Information is not deleted in the original web site.

-Delisting exclusively affects information which is not of interest for the general public.

-In exceptional cases where results containing information of interest for the public is delisted because of reasons related to its special sensitivity for the private life of the affected data subject, the impact is still limited (on account of the accessibility of the information following other search criteria and on the original web site) and the strictly necessary to safeguard the rights of the data subject.

(f) Editors of original web pages play no role within the assessment procedure, also for different reasons:

- The assessment of the different rights and interests corresponds to the search engine in its role as data controller of a processing operation which is different and independent from processing operations carried out by web publishers.

- Participation of web editors in delisting decisions would only be necessary and acceptable if they could adduce that their rights or interests are affected.

- The CJUE limits the content of the assessment required to make decisions to the rights of data subject and the interest of the general public in having access to the information via the search engine. Web editors are not taken into consideration.

- There is nothing such as a “right to be indexed” or a “legitimate interest” in being indexed. Search engines are not bound to editors by contractual conditions. Search engines collect the information, and present it to their users in response to queries, according to their own criteria, priorities and policies. Editors cannot request search engines to be indexed or that results concerning information they have uploaded is displayed in a specific manner or position. As far as we know, there are no precedents of legal actions of editors requesting compensation for not being indexed or for being treated in an “unfair” way by search engines.

(g) Consequently, the participation of editors in the process would not be supported by the defense of a right or a legitimate interest. However, it cannot be excluded that, exceptionally and in specific cases, search engines may be obliged to consult editors in order to obtain additional information that may be necessary in order to properly carry out the assessment of the circumstances of the case.

(h) Additionally, making it compulsory for search engines to contact editors as a rule in the assessment of all requests they receive would imply an excessive burden and could unnecessarily slow down the procedure.

FOURTH.- The establishment of special mechanisms aimed at ensuring the proper implementation of a “right to be forgotten” is not necessary and might be counterproductive.

(a)The so called “right to be forgotten” is just the exercise of the rights to erasure and to object vis à vis search engines. As such, the procedures to assess the circumstances of each request and the supervision of the conduct of the controllers should be the same that are generally used.

(b) As web editors cannot adduce any right nor any legitimate interest in the assessment of the rights and interests at stake, there is no reason to devise mechanisms that may allow for those rights to be taken into consideration.

(c) The implementation of these rights may be monitored by DPAs in the same way that they supervise the activity of any data controller. This supervision is not necessarily the consequence of a complaint and may be exercised in procedures started “ex officio” by DPAs.

FRANCE

I. Collective Actions - Article 76

The French authorities consider that collective claims lodged by associations, organisations or bodies on their own initiative and without the data subjects' mandate represent the only effective method of grouping together small-scale individual actions against major controllers or processors, by allowing individuals to join as parties to a claim lodged by an association (or by any other body having capacity according to national law), particularly on the association's appeal.

Given that breaches of data protection rules can have serious consequences, potentially affecting many individuals when committed by certain major operators, the extension of collective claims - already used in various Member States in the area of consumer protection - to this type of dispute is particularly welcome.

The creation of this type of claim is also a logical consequence of the accountability of companies which the proposal for a Regulation seeks to achieve, and which governs the risk-based approach.

However, Article 76(1a) currently only allows this type of claim to be submitted to supervisory authorities, which limits the usefulness of the procedures considerably.

We would therefore like this Article to be supplemented to oblige Member States to enact in national law, in accordance with the principle of procedural autonomy, the possibility for associations, bodies and organisations to take action before supervisory authorities or the courts, whether or not they have the data subjects' mandate, at least in order to stop infringements of the Regulation. This is also a major issue in terms of harmonising the protection afforded to data subjects within the European Union, and a method of combating forum shopping more effectively.

The introduction of this type of collective claim would mean the Regulation would bring real added value in terms of protecting the rights of individuals by making it easier for them to defend their rights, as was highlighted by the Article 29 Working Party in its contribution of 1 December 2009.

We would therefore like this Article to be amended, and for Article 76(1a) to be redrafted as follows:

1a. ***Member States shall provide adequate and effective legal remedies for*** *any body, organization or association referred to in paragraph 1, independently of a data subject's mandate or complaint,* ***and for rules to ensure that they have the right to a judicial remedy against a controller or processor, at least to ensure full implementation of this regulation.***

II. Remedies and liability of controllers and processors - Article 77

We do not wish to challenge the principle of accountability of processors that has already been agreed in Chapter IV, which imposes specific obligations on processors and obliges them to follow the instructions given by the controller.

However, we do set great store by the protection of individuals under the systems for remedies and liability provided for in the Regulation.

That is why we would nonetheless like the processor(s) to be held potentially liable where the processor has not complied with the specific obligations incumbent on it pursuant to the Regulation, or where it has acted outside the scope of the instructions given by the controller.

However, we are also keen to ensure sufficient legal certainty for companies, controllers and processors. Article 77 as currently drafted, providing that controllers and processors are jointly and severally liable, would lead them to make provisions for risks, and consequently to price increases, without the data subject gaining any significant benefit, even though the principle of joint liability between the controller and the processor is already established.

We would therefore like the wording of this Article to be amended:

- to provide for joint liability only between the controller and the processor(s) by deleting the words "and severally" from paragraph 2;

- to avoid paragraph 3 having the effect of exempting the controller or the processor from liability only if they prove that they are not at all responsible for the event or act giving rise to the damage.

Furthermore, we consider it essential to clarify that the processor can only be held liable for those obligations which are directly incumbent upon them pursuant to the Regulation, or where they act in a way that is contrary to or outside the scope of the instructions of the controller. In this respect, recital 118 should also clarify this point.

Finally, we recognise that in certain situations, the processor could find themselves in a strong position in relation to the controller. This is why we also suggest introducing the following mechanism: where the controller uses certified processors, this certification will result in a transfer of liability from the controller to the processor in relation to those activities covered by the certification. Using certification will allow companies to benefit from greater legal certainty, thereby encouraging them to make use of it, whilst at the same time providing a guarantee to data subjects that their data will be processed according to procedures that comply with the Regulation.

Article 77(2)

"2. 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 ***~~and~~ ~~severally~~*** *liable for the entire amount of the damage This is without prejudice to recourse claims between controllers and/or processors."*

Article 77(3)

"3. The controller or the processor ***~~may~~ shall*** *be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not* ***responsible, in whole or in part,*** *for the event giving rise to the damage.* ***When the processing of the controller relies on a service provided by a certified processor, in accordance with article 39, this processor shall be solely liable if the damage results from its certified processing activities."***

Recital 118

"*Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who* ***~~may~~*** ***should*** *be exempted from liability if they prove that they are not responsible for the damage, in particular where* ***~~he~~ they*** *establish****~~es~~*** *fault on the part of the data subject or in case of force majeure.* ***The processor should not be exempted if the damage results, in whole or in part, either from the fact that he has not complied with the instructions of the controller or if the damage results in whole or in part from a personal data breach on his part.***"

CROATIA

No. 7526/15

Article 12 - Transparent information, communication and modalities for exercising the rights for the data subject

We think it is necessary to maintain a fixed deadline for reasons of predictability of procedure (one month with the obligation of controller to provide information without undue delay). Further to paragraph 4 we propose to retain the existing expression (*manifestly unfounded*).

Article 14 - Information to be provided where the data are collected from the data subject

We propose to retain the existing expression without adding the suggested, as it will go below the level of protection laid down in Directive 1995. Further to paragraph 1 (b) the proposed addition of expression *and of compatible further processing* can be supported, but with clearer definition of what exactly is meant by further compatible data processing.

Article 14a - Information to be provided where the data have not been obtained from the data subject

We would like to keep those points for the reasons specified in national legislation of MS.

Article 17 – The right to be forgotten and erasure

HR consider that the right to be forgotten is an added value of the Draft Regulation, and we believe that should be taken into consideration that is broader than just the right for erasure, and that has been recognized in the jurisprudence. We can support the FR proposal relating to the protection of children's rights.

Article 17 - The right to be forgotten and dispute settlement

To the DE proposal of the specific model for resolving disputes that involve Internet browsers, we believe that this solution is not necessary, as it would seem unnecessary distinction between them and other controllers.

Article 18 – Data portability

We believe that it is necessary to also include an obligation for the controller to transmit the data to another controller or third party in the context of data portability, and that the right is extend to public authorities, except in cases where such portability of personal data are in contrary to the processing (for example if data subject asks to submit their personal data of classified nature).

Article 19 - The right to object

It is proposed to keep the existing text without specifying the reference to Article 6 (1), paragraph (e). FR proposal can be supported because it strengthens the legal protection of data subjects.

Article 20 - Profiling

We consider that the profiling based on the automatic machine deciding is unacceptable without human intervention due to, inter alia, discriminatory effects (supported by HU). We can support the expression used in the definitions.

Article 76 - Representation of data subjects

According to the Croatian Law on Personal Data Protection the request for protection of rights may be submitted by the data subject himself or by his representative, so we are unable to support the option provided in paragraph 1a.

Article 77 - Right to compensation and liability

As regard to the responsibilities of data controller and data processor, we point out that according to Croatian regulations data controller is responsible for all processing of personal data and the data processor is responsible for his segment of processing of personal data. Therefore, we suggest that the first instance is to address to data controller.

Article 79b - Penalties

We can support expression *may* in the article, given that it enables the MS to prescribe provisions in the national legislation which may be of criminal or administrative character.

No. 7084/15

In regard to recital 54aa) we suggest adding in the second sentence:

54aa)(...) *This may lead to the result that the personal data has to be maintained for exercising the right of freedom of expression, when required by law, for archiving purposes in the public interest or for historical, statistical and scientific (...) purposes, for reasons of public interest in the area of public health or social protection, or for the establishment, exercise or defence of legal claims*, **having in mind the fair balance stipulated in Recital 53a) and the personal data is not in the contradiction with the fundamental rights and freedoms of data subjects.**

NETHERLANDS

NL suggestions on Chapter III and VIII

Article 14

Information to be provided where the data are collected from the data subject[1]

1[2]. Where personal data relating to a data subject are collected from the data subject, the controller shall (…), at the time when personal data are obtained, provide the data subject with the following information:

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

(b) the purposes of the processing for which the personal data are intended (…).

[1] DE, EE, ES, NL, SE, FI, PT and UK scrutiny reservation. DE, supported by ES and NL, has asked the Commission to provide an assessment of the extra costs for the industry under this provision.

[2] HU thought the legal basis of the processing should be included in the list.

1a. In addition to the information referred to in paragraph 1, the controller shall[3] where appropriate provide the data subject with such further information [4]necessary to ensure fair and transparent processing in respect of the data subject[5], having regard to the specific circumstances and context in which the personal data are processed[6]:

(a) (…);

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller **or by a third party, the interests, fundamental rights and freedoms of the data subjects concerned and the result of the weighing of these interests, pursuant to Article 6 (1), point (f);**

(c) the recipients or categories of recipients of the personal data[7];

(d) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation;

(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data or restriction of processing of personal data concerning the data subject and to object to the processing of such personal data (…)[8];

---

3 DE, EE, and PL asked to insert "on request". DE, DK, NL and UK doubted whether the redraft would allow for a sufficient risk-based approach and warned against excessive administrative burdens/compliance costs. DK and UK in particular referred to the difficulty for controllers in assessing what is required under para. 1a in order to ensure fair and transparent processing. DE, EE and PL pleaded for making the obligation to provide this information contingent upon a request thereto as the controller might otherwise take a risk-averse approach and provide all the information under Article 14(1a), also in cases where not required. UK thought that many of the aspects set out in paragraph 1a of Article 14 (and paragraph 2 of Article 14a) could be left to guidance under Article 39.

4 CZ suggested adding the word 'obviously'.

5 FR scrutiny reservation.

6 COM reservation on deletion of the words 'such as'.

7 AT and DE thought that this concept was too vague (does it e.g. encompass employees of the data controller?).

8 The reference to direct marketing was deleted in view of comments by DK, FR, IT and SE.

[9]

(f) the right to lodge a complaint to a supervisory authority (…);

(g) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as **whether the data subject is obliged to provide the data and of** the possible consequences of failure to provide such data[10];

(h) *the existence of* **automated decision making including** *-profiling referred to in Article 20(1) and (3) and information concerning* (…) *the* ***processing****, as well as the significance and the envisaged consequences of such* ***processing*** *for the data subject.* [11]

1b. Where the controller intends to process the data in accordance with Article 6, (3), (3a) and (4) for another purpose than the one for which the data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 1a.

2. (…)[12]

3. (…)

4. (…)

5. Paragraphs 1, 1a and 1b shall not apply where and insofar as the data subject already has the information.

---

9 NL considers that Art. 14 para 1 (ea) is already covered in Art. 7, para 3.
10 CZ, DE, ES and NL reservation.
11 SE scrutiny reservation.
12 HU reservation on the deletion of this paragraph.

Article 14 a

Information to be provided where the data have not been obtained

***from the data subject*[13]**

1[14]. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

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

(b) the purposes of the processing for which the personal data are intended.

2. In addition to the information referred to in paragraph 1, the controller shall where appropriate provide the data subject with such further information necessary to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context[15] in which the personal data are processed (…):

(a) the categories of personal data concerned;

(b) (…)

(c) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller **or by a third party, the interests, fundamental rights and freedoms of the data subjects concerned and the result of the weighing of these interests, pursuant to Article 6 (1), point (f)**;

(d) the recipients or categories of recipients of the personal data;

---

13 DE, EE, ES, NL (§§1+2),AT, PT scrutiny reservation.

14 HU thought the legal basis of the processing should be included in the list.

15 ES, IT and FR doubts on the addition of the words 'and context'.

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

(ea) where the processing is based on point (a) of Article 6(1), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(f) the right to lodge a complaint to a supervisory authority (…);

(g) the origin of the personal data, unless the data originate from publicly accessible sources[16];

*(h) the existence of **automated decision making including** profiling referred to in Article 20(1) and (3) and information concerning (...) the **processing**, as well as the significance and the envisaged consequences of such **processing** for the data subject.*[17]

3. The controller shall provide the information referred to in paragraphs 1 and 2[18]:

(a) within a reasonable period after obtaining the data, having regard to the specific circumstances in which the data are processed, or

(b) if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed.

---

16 COM and AT scrutiny reservation.

17 PL asks for the deletion of the reference to 'logic'.

18 BE proposed to add: 'possibly through an easily accessible contact person where the data subject concerned can consult his data'. This is already covered by the modified recital 46.

3a **Where the controller intends to process the data in accordance with Article 6 (3), (3a) and (4) for another purpose than the one for which the data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.**

4. Paragraphs 1 to 3 shall not apply where and insofar as:

(a) the data subject already has the information; or

(b) the provision of such information **(…)** proves impossible or would involve a disproportionate effort or is likely to render impossible or to seriously impair the achievement of the purposes of the processing[19]; in such cases the controller shall take appropriate measures to protect the *data subject's* **rights and freedoms and** legitimate interests[20]; or

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests[21]; or

(d) where the data originate from publicly available sources[22]; or

(e) where the data must remain confidential in accordance with a legal provision in Union or Member State law or because of the overriding legitimate interests of another person[23].

---

19 COM scrutiny reservation.

20 Several delegations (DE, DK, FI, PL, SK, and LT) thought that in this Regulation (contrary to the 1995 Directive) the text should be specified so as to clarify both the concepts of 'appropriate measures' and of 'legitimate interests'. According to the Commission, this should be done through delegated acts under Article 15(7). DE warned that a dangerous situation might ensue if these delegated acts were not enacted in due time.

21 UK thought the requirement of a legal obligation was enough and no further appropriate measures should be required.

22 COM, IT and FR reservation on this exception. ES thought this concept required further clarification. DE and SE emphasised the importance of this exception.

23 COM and AT reservation on (d) and (e). UK referred to the existence of case law regarding privilege (confidentiality). BE thought the reference to the overriding interests of another person was too broad.

5. (…)

6. (…)

Article 16

Right to rectification[24]

1. (…) The data subject shall have the right[25] to obtain from the controller the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary (…) statement.

2. **(…)**[26]

[24] DE and UK scrutiny reservation.

[25] UK suggested to insert the qualification ' where reasonably practicable' UK also suggested inserting the qualification 'where necessary'.

[26] Deleted in view of the new Article 83.

Article 17

Right to be forgotten and to erasure[27]

1. The (…) controller shall have the obligation to erase personal data without undue delay and the data subject shall have the right to obtain the erasure of personal data **concerning him or her** without undue delay 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;

[27] DE, EE, PT, SE, SI, FI and UK scrutiny reservation. EE, FR, NL, RO and SE reservation on the applicability to the public sector. Whereas some Member States have welcomed the proposal to introduce a right to be forgotten (AT, EE, FR, IE); other delegations were more sceptical as to the feasibility of introducing a right which would go beyond the right to obtain from the controller the erasure of one's own personal data (DE, DK, ES). The difficulties flowing from the household exception (UK), to apply such right to personal data posted on social media were highlighted (BE, DE, FR), but also the impossibility to apply such right to 'paper/offline' data was stressed (EE, LU, SI). Some delegations (DE, ES) also pointed to the possible externalities of such right when applied with fraudulent intent (e.g. when applying it to the financial sector). Several delegations referred to the challenge to make data subjects active in an online environment behave responsibly (DE, LU and UK) and queried whether the creation of such a right would not be counterproductive to the realisation of this challenge, by creating unreasonable expectations as to the possibilities of erasing data (DK, LU and UK). Some delegations thought that the right to be forgotten was rather an element of the right to privacy than part of data protection and should be balanced against the right to remember and access to information sources as part of the freedom of expression (DE, ES, LU, NL, SI, PT and UK). It was pointed out that the possibility for Member States to restrict the right to be forgotten under Article 21 where it interferes with the freedom of expression is not sufficient to allay all concerns in that regard as it would be difficult for controllers to make complex determinations about the balance with the freedom of expression, especially in view of the stiff sanctions provided in Article 79 (UK). In general several delegations (CZ, DE, FR) stressed the need for further examining the relationship between the right to be forgotten and other data protection rights. The Commission emphasised that its proposal was in no way meant to be a limitation of the freedom of expression. The inherent problems in enforcing such right in a globalised world outside the EU were cited as well as the possible consequences for the competitive position of EU companies linked thereto (BE, AT, LV, LU, NL, SE and SI).

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) or point (a) of Article 9(2) and (…) there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data and has made a specific request to obtain erasure of the data *pursuant to Article 19(1)* and there are no overriding legitimate grounds for the processing or the data subject objects to the processing of personal data pursuant to Article 19(2);

(d) the data have been unlawfully processed[28];

(e) the data have to be erased for compliance with a legal obligation to which the controller is subject[29] [30].

2. (…).

[28] UK scrutiny reservation: this was overly broad.

[29] RO scrutiny reservation.

[30] DE pointed to the difficulties in determining who is the controller in respect of data who are copied/made available by other controllers (e.g. a search engine) than the initial controller (e.g. a newspaper). AT opined that the exercise of the right to be forgotten would have take place in a gradual approach, first against the initial controller and subsequently against the 'secondary' controllers. ES referred to the problem of initial controllers that have disappeared and thought that in such cases the right to be forgotten could immediately be exercised against the 'secondary controllers' ES suggested adding in paragraph 2: 'Where the controller who permitted access to the personal data has disappeared, ceased to exist or cannot be contacted by the data subject for other reasons, the data subject shall have the right to have other data controllers delete any link to copies or replications thereof'. The Commission, however, replied that the right to be forgotten could not be exercised against journals exercising freedom of expression. According to the Commission, the indexation of personal data by search engines is a processing activity not protected by the freedom of expression.

2a. *Where the controller*[31] *(...) has made the personal data public*[32] *and is obliged pursuant to paragraph 1 to erase the data,* the controller, taking account of available technology and the cost of implementation[33], *shall take (...) reasonable steps*[34], *including technical measures, (...) to inform* **known** *controllers*[35] *which are processing* the *data, that a data subject requests them to erase any links to, or copy or replication of that personal data*[36].

---

31 BE, DE and SI queried whether this also covered controllers (e.g. a search engine) other than the initial controller (e.g. a newspaper).

32 ES prefers referring to 'expressly or tacitly allowing third parties access to'. IE thought it would be more realistic to oblige controllers to erase personal data which are under their control, or reasonably accessible to them in the ordinary course of business, i.e. within the control of those with whom they have contractual and business relations. BE, supported by IE and LU, also remarked that the E-Commerce Directive should be taken into account (e.g. through a reference in a recital) and asked whether this proposed liability did not violate the exemption for information society services provided in that Directive (Article 12 of Directive 2000/31/EC of 8 June 2000), but COM replied there was no contradiction. LU pointed to a risk of obliging controllers in an online context to monitor all data traffic, which would be contrary to the principle of data minimization and in breach with the prohibition in Article 15 of the E-Commerce Directive to monitor transmitted information.

33 Further to NL suggestion. This may hopefully also accommodate the DE concern that the reference to available technology could be read as implying an obligation to always use the latest technology;

34 LU queried why the reference to all reasonable steps had not been inserted in paragraph 1 as well and SE, supported by DK, suggested clarifying it in a recital. COM replied that paragraph 1 expressed a results obligation whereas paragraph 2 was only an obligation to use one's best efforts. ES thought the term should rather be 'proportionate steps'. DE, ES and BG questioned the scope of this term. ES queried whether there was a duty on controllers to act proactively with a view to possible exercise of the right to be forgotten. DE warned against the 'chilling effect' such obligation might have on the exercise of the freedom of expression.

35 BE, supported by ES and FR, suggested referring to 'known' controllers (or third parties).

36 BE and ES queried whether this was also possible for the offline world and BE suggested to clearly distinguish the obligations of controllers between the online and offline world. Several Member States (CZ, DE, LU, NL, PL, PT, SE and SI) had doubts on the enforceability of this rule.

3. Paragraphs 1 and 2a shall not apply[37] to the extent that (…) processing of the personal data is necessary:

a. for exercising the right of freedom of expression in accordance with Article 80[38];

b. for reasons of public interest in the area of public health in accordance with Article **9(2)(g)(h) and (hb) as well as Article 9(4)**[39];

c. for archiving purposes in the public interest or for *scientific, statistical* **and** historical (…) purposes in accordance with **Article 83**;

d. (…)

e. (…)

f. for the establishment, exercise or defence of legal claims.

[37] DE queried whether these exceptions also applied to the abstention from further dissemination of personal data. AT and DE pointed out that Article 6 contained an absolute obligation to erase data in the cases listed in that article and considered that it was therefore illogical to provide for exception in this paragraph.

[38] DE and EE asked why this exception had not been extended to individuals using their own freedom of expression (e.g. an individual blogger).

[39] DK queried whether this exception implied that a doctor could refuse to erase a patient's personal data notwithstanding an explicit request to that end from the latter. ES and DE indicated that this related to the more general question of how to resolve differences of view between the data subject and the data controller, especially in cases where the interests of third parties were at stake. PL asked what was the relation to Article 21.

4. Paragraphs 1 and 2a shall not apply when the processing of the personal data is necessary for compliance with a legal obligation to process the personal data pursuant to Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

5. (…)

AUSTRIA

CHAPTERS III and VIII (Doc. 7084/15)

Preliminary the Austrian delegations would like to suggest the following amendments to Chapter III (Doc. 7084/15). The recitals have to be adapted accordingly. Provisions not mentioned in the following text are meant to be unchanged for the time being. Changes are in *bold, italic and underlined*.

Article 12
Transparent information, communication and modalities for exercising the rights of the data subject

1. The controller shall ***take appropriate measures to*** provide any information referred to in Articles 14 and 14a and any communication under Articles 15 to 19 and 32 relating to the processing of personal data to the data subject in ***an easily accessible form and intelligible***, using clear and plain language ***adapted to the data subject***. The information shall be provided in writing***, or where appropriate, electronically or by other means***. ***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. When requested by the data subject the information may be given orally provided that the identity of the data subjects is proven.***

2. The controller shall provide the ***information referred to in Articles 14a and 15 and*** information on action taken on a request under Articles ***15*** to 19 to the data subject without undue delay and at the latest within one month of receipt of the request (…). This period may be extended for a further two months when necessary, taking into account the complexity of the request and the number of requests. Where the extended period applies, the data subject shall be informed within one month of receipt of the request of the reasons for the delay.

4. Information provided under Articles 14 and 14a (…) and any communication under Articles 16 to 19 and 32 shall be provided free of charge. Where requests from a data subject are *manifestly* unfounded or excessive, in particular because of their repetitive character, the controller (…) may refuse to act on the request. In that case, the controller shall bear the burden of demonstrating the *manifestly* unfounded or excessive character of the request. ***The controller shall inform the data subject of the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy***.

Request of an additional recital for Art. 12 para 4a (identification of the data subject):

There should be no doubt about the fact that as a general rule a user when relying particularly on his/her right of access or deletion should not be required to provide the controller with more information about himself/herself that the latter already holds. Within the context of a request for access directed to a mail provider e.g. it should last that the user identifies himself/herself by its account ("user ID") in combination with a password.

Article 14

Information to be provided where the data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall (…), at the time when personal data are obtained, provide the data subject with the following information:

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

(c) the legal basis for which the personal data are intended;

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

(e) the right to lodge a complaint to a supervisory authority (…);

1a. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with such further information necessary to ensure fair and transparent processing in respect of the data subject, ***~~having regard to the specific circumstances and context in which the personal data are processed~~ such as***:

(a) the period for which the personal data will be stored, or if this is impossible, the criteria used to determine this period

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

~~(f) the right to lodge a complaint to a supervisory authority (…);~~

5. Paragraphs 1, ***1a and 1b*** shall not apply where and insofar as the data subject already has the information.

Article 14a

Information to be provided where the data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(c) the legal basis for which the personal data are intended.

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

(e) the right to lodge a complaint to a supervisory authority (…);

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with such further information necessary to ensure fair and transparent processing in respect of the data subject, ~~***having regard to the specific circumstances and context in which the personal data are processed such as***~~ ***such as***:

(b) the period for which the personal data will be stored, or if this is impossible, the criteria used to determine this period

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

~~***(f) the right to lodge a complaint to a supervisory authority (…);***~~

(g) the origin of the personal data, ~~***unless the data originate from publicly accessible source***~~s;

4. Paragraphs 1 to ***3a*** shall not apply where and insofar as:

(b) the provision of such information **(…)** proves impossible or would involve a disproportionate effort ~~***or is likely to render impossible or to seriously impair the achievement of the purposes of the processing; in such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests;***~~ or

~~***(d) where the data originate from publicly available sources; or***~~

~~***(e)***~~ where the data must remain confidential in accordance with a legal provision in Union or Member State law ~~***or because of the overriding legitimate interests of another person39.***~~

Article 15

Right of access for the data subject

1. The data subject shall have the right to obtain from the controller at reasonable intervals and free of charge (…) confirmation as to whether or not personal data concerning him or her are being processed and where such personal data are being processed access to the data and the following information:

(aO) the personal data undergoing processing

(a) the purposes ***and the legal basis*** of the processing;

(d) the period for which the personal data will be stored, or if this is impossible, the criteria used to determine this period

1b. ~~On request and without an excessive charge,~~ The controller shall provide a copy of the personal data undergoing processing to the data subject. The information shall be given free of charge if it concerns the current data files of a use of data and if the person requesting information has not yet made a request for information to the same controller regarding the same application purpose in the current year. In all other cases a flat rate compensation may be charged; deviations are permitted to cover actually incurred higher expenses.

1c. Upon inquiry, the person requesting information has to cooperate in the information procedure to a reasonable extent to prevent an unwarranted and disproportionate effort on the part of the controller.

2. Where personal data supplied by the data subject are processed by automated means ***~~and in a structured and commonly used format~~***, the controller shall, on request and without an excessive charge, provide a copy of the data concerning the data subject ***in a structured and commonly used format*** to the data subject.

2a. The right to obtain a copy referred to in paragraphs ***~~1b and~~*** 2 shall not apply where such copy cannot be provided without disclosing personal data of other data subjects.

Article 17

Right to erasure

1. The (…) controller shall have the obligation to erase personal data without undue delay and the data subject shall have the right to obtain the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) or point (a) of Article 9(2) and (…) there is no other legal ground for the processing of the data;

The question here is whether this last sentence is linked to the notion of further processing. This has to be clarified in a recital.

(d) the data have been unlawfully processed;

A recital has to clarify that not any infringement of the regulation leads to the right to erasure. For example in a situation where personal data are processed in accordance with Art. 6 (1) (c) and the controller doesn´t inform the data subject in accordance with Art. 14 or 14a the right to erasure shall not apply.

2a. Where the controller (…) has made the personal data public and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, shall take (…) reasonable steps, including technical measures, (…) to inform known controllers which are processing the data, that a data subject requests them to erase any links to, or copy or replication of that personal data.

3. Paragraphs 1 ***and 2a*** shall not apply to the extent that (…) processing of the personal data is necessary:

(a) for exercising the right of freedom of expression in accordance with Article 80;

(d) for archiving purposes in the public interest or for scientific, statistical and historical (…) purposes in accordance with Article 83;

Article 17c

Right to be forgotten

1. [A basic provisions has to be added implementing of ECJ Google judgment.]

2. Where the controller (…) has made the personal data public and is obliged pursuant to Article 17 paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, shall take (…) reasonable steps, including technical measures, (…) to inform ~~known~~ controllers which are processing the data, that a data subject requests them to erase any links to, or copy or replication of that personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that (…) processing of the personal data is necessary:

(a) for exercising the right of freedom of expression in accordance with Article 80;

Further discussion and complementing recitals are essential and needed.

SECTION 4

RIGHT TO OBJECT *AND AUTOMATED DECISION MAKING*

Article 20

Automated decision making

The provision is closely linked to the definitions in Art. 4 and has to be read together. In any case we have to avoid the linkage between profiling and other instruments like data mining or big data.

Further discussion and complementing recitals on Article 20 are essential and needed.

CHAPTER VIII
REMEDIES, LIABILITY AND SANCTIONS

The further remark is limited to Art. 75. We will provide further comments in due course.

Article 75
Right to a judicial remedy against a controller or processor

Para 1 should read as follows:

1. ***Insofar as a supervisory authority cannot itself take a binding decision on a complaint****, a data subject shall have the right to an effective judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.*

Justification:

This is intended to take account of cases where a Member State establishes its national supervisory authority in such a way that in certain exceptional circumstances it is unable to take any legally binding decisions for or against the interests of data subjects. This is the only instance in which there is any point in providing direct access to a court without the supervisory authority having to act first or issue a (non-binding) decision. However, where this does not apply, full parallelism between the legal protection afforded by the supervisory authorities and the courts is not logically conceivable.

Art. 22 of the Directive 95/46/EC has been understood that various possibilities for implementation are available to the Member States. A Member State may

- establish the data protection authority itself as a "court", or

- provide a court (with full knowledge of the facts) as an authority above the supervisory authority (judicial remedy)

or

- establish the supervisory authority as an ombudsman-like body which does not "decide". In that case only the court takes legally binding decisions and is especially not bound by the opinion of the supervisory authority.

However, the rules in the Directive have not been understood to require that a court also may decide a case where the supervisory authority has the power to take decisions. This would be illogical since it would cause an insolvable conflict between legal acts issued on one hand by the supervisory authority and on the other hand by the court seized.

Art. 75 of the Regulations is now creating the same problem if it has to be understood to offer the right to genuine choice between the different judicial remedies.
In our understanding we have to achieve the following solution:

a) where a supervisory authority has the power to take binding decisions a court can only have the power to review the decision by the supervisory authority;
b) where the supervisory authority deals with a case without having the power to take a binding decision the data subject is in fact free to choose whether to bring a court action immediately (instead of) or during or after the end of the proceedings before the supervisory authority.

Genuinely parallel proceedings have to be avoided.

POLAND

Poland's comments on Chapters III (following the DAPIX meeting 23-24.03.2015: doc: 7084/15 DATAPROTECT 31 JAI 169 MI 159 DRS 23 DAPIX 39 FREMP 50 COMIX 114 CODEC 336).

Proposed changes to the text are marked in **bold**. The changes should be read together with our interventions during the DAPIX meeting of 23-24.03.2015.

CHAPTER III

Art.12 - Transparent information, communication and modalities for exercising the rights of the data subject

Poland supports introduction of adjective "abusive" in Art. 12.4:

> *4. Information provided under Articles 14 and 14a (...) and any communication under Articles 16 to 19 and 32 shall be provided free of charge. Where requests from a data subject are* ***abusive*** ~~***manifestly unfounded or excessive***~~*, in particular because of their repetitive character, the controller (...) may refuse to act on the request. In that case, the controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.*

Art. 14 - Information to be provided where the data are collected from the data subject

- Poland would like to underline that overloading a data subject with information may lead to situation where information provided by a data controller would not be clear for him/her

- Poland supports new par. 1b (which makes the control of data subject over their data more effective).

- We believe that when a DPO is appointed, a data controller should be obliged to provide DPO's contact details at the time when personal data are obtained:

1. Where personal data relating to a data subject are collected from the data subject, the controller shall (...), at the time when personal data are obtained, provide the data subject with the following information:

*(a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller **~~may~~ shall** also include the contact details of the data protection officer, if any;*

(...)

- Poland believes that information duty should not apply when provision of information proves to be impossible or would involve a disproportionate effort. Such an approach is in line with Directive 95/46:

*5. Paragraphs 1, 1a **and 1b** shall not apply where and insofar as:*

(a) the data subject already has the information; or

***(b) the provision of such information (…) proves impossible or would involve a disproportionate effort; in such case the controller shall take appropriate measures to protect the data subject's rights and freedoms**.*

Art. 14a - ***Information to be provided where the data have not been obtained from the data subject***

- **Footnote 33** – Poland withdraws the comment from footnote 33, as they were taken into consideration by the PRES.

- Poland **supports new par. 3a**, which makes control of data subjects over their data more effective.

- We believe that reference to "or to seriously impair the achievement of the purposes of the processing" in Art. 14a should be deleted, as data controller's purposes should not override his/her information duty:

*4. Paragraphs 1 to **3a** shall not apply where and insofar as:*

(a) the data subject already has the information; or

*(b) the provision of such information **(…)** proves impossible or would involve a disproportionate effort or is likely to render impossible ~~**or to seriously impair the achievement of the purposes of the processing**~~; in such **a cases** ~~**a**~~ the controller shall take appropriate measures to protect the data subject's **rights and freedoms and legitimate interests**; or*

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the data originate from publicly available sources; or

(e) where the data must remain confidential in accordance with a legal provision in Union or Member State law or because of the overriding legitimate interests of another person.

- **Footnote 39:** PL asks to be added (together with BE) to footnote 39 (the term „overriding legitimate interests of another person" is too broad and should be narrowed).

Art.15 - Right of access for the data subject

- Par. 1 point (h) should be changed as follows:

"in the case of automated decision making including profiling referred to in Article 20(1) and (3), information concerning (...) the processing as well as the significance and envisaged consequences of such processing"

Art.17 - Right to be forgotten and to erasure

- Poland would like to narrow the scope of Art. 17 par 2a, in order to make "right to be forgotten" possible to be implemented in practice. The initial proposal of the EC, from Polish perspective seems to be unrealistic:

2a. *Where the controller (…) has made the personal data public* *and is obliged pursuant to paragraph 1 to erase the data,* the controller, taking account of available technology and the cost of implementation, *shall take (…) reasonable steps, including technical measures, (…) to inform* ~~**known**~~ *controllers* **to which he intentionally disclosed** ~~***which are processing***~~ *the data, that a data subject requests them to erase any links to, or copy or replication of that personal data.*

- **Recital 53a:** Poland proposes the following wording:

Inasmuch as the removal of links from the list of internet search results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information ***as well as this right should be considered in relation to the fundamental right to freedom of expression****, a fair balance should be sought in particular between* ~~***that***~~ *interest* ***in having access to that information, the right to freedom of expression provided in Article 11 of the Charter*** *and the data subject's fundamental rights under Articles 7 and 8 of the Charter.* ~~***Whilst the data subject's rights protected by those articles should override, as a general rule, the interest of internet users,***~~ ***T****hat balance may in specific cases depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having access to that information, an interest which may vary, in particular, according to the role played by the data subject in public life.*

Comment: the right to erasure and the right to be forgotten cannot undermine the principle of freedom of expression which is also one of fundamental rights provided in the Charter, and these two rights (right to privacy and freedom of expression and information) should be treated equally.

- **Recital 54aa:** Poland proposes the following wording:

54aa) However the right to be forgotten should be balanced with other fundamental rights. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. This may lead to the result that the personal data has to be maintained for exercising the right of freedom of expression, ~~***when required by law***~~*, for archiving purposes in the public interest or for historical, statistical and scientific (…) purposes, for reasons of public interest in the area of public health or social protection, or for the establishment, exercise or defence of legal claims.*

Comment: Freedom of expression does not require a legal basis in order to be balanced with conflicting rights, therefore the passage “when required by law” in Recital 54aa has to be deleted.

Art. 17b - Notification obligation regarding rectification or erasure

- Poland supports the position of BE, ES, FR in the **footnote 77** on the need to limit the scope of this article to the "known recipients". At the same time, Poland points on the possible negative effects of informing all recipients ("each recipient”) because in certain situations, this can have negative consequences for the data subjects (eg. giving additional information concerning the data subject, which recipient might had already forgotten) here, in this regard, we also support DE in **footnote 76.**

Art. 20 - Decisions based on profiling

- Decisions based on profiling should be allowed, but it must be carried out in a transparent and nondiscriminatory manner. A person who is subject to profiling should receive adequate information before profiling.

- It is also important to differentiate the situations when we deal with profiling, within a meaning of a form of automated processing, but when no decision which might produce legal effects or significantly affect the natural person is taken, from the situations when profiling is used to take decision which produces legal effects or significantly affects the natural person. In the first situation, the activity of automated processing or profiling itself should be allowed and be subject only to the general rules governing processing of personal data.

- At the same time, in **par. 1** the word “***solely***” should be deleted which would make the application of this provision too broad – each decision – making which is based not only, but – *inter alia* – on automated processing should be subject to requirements of this provision. In most cases, for example when the assessing of credit worthiness, the automated processing is only one, but non sole of the operations:

*1. **The** data subject shall have the right not to be subject to a decision **evaluating personal aspects relating to him or her, which is** based **~~solely~~ on automated processing, including** profiling**, and** produces legal effects concerning him or her or **significantly** affects him or her.*

POLAND – COMMENTS ON CHAPTER VIII

Art. 74 - Right to an effective judicial remedy against a supervisory authority

Art. 75 - Right to a judicial remedy against a controller or processor

- According to Poland, in principle, every judicial remedy should be "effective" by its definition, therefore Poland wonders whether there is a necessity to use the adjective "effective" in this context in Art. 74 and Art. 75.

Art. 76 - Representation of data subjects

- Poland is against empowering a body, organisation or association with a right to lodge a complaint independently. Bodies, organisations or associations referred to in par. 1 should, in case they gain knowledge about possible breach, inform relevant DPA, which in such situation is obliged to investigate the case ex officio. In such a case it is the role of a DPA to take action, if needed. Moreover, if a data subject wants to be represented by an organisation, he or she may issue a power of attorney authorising relevant body organisation or association to act on his or her behalf. Therefore, Poland is in favour of deletion of par. 1a.

Art. 76a - Suspension of proceedings

- In Poland's opinion the proposed mechanism still needs to be further developed and clarified. In particular, it can be difficult to exchange information between courts of different Member States and coordinate their actions as well as to force national courts to suspend proceedings, when waiting for another national court's ruling. Moreover, the provision does not regulate the situations when, for example, both national courts suspend their proceedings, stating that the other court is competent to issue ruling in a particular case.

- The explanation of the term "the same processing activities" is needed, in particular it is not clear whether this term refers to: (i) the cases that have the same scope; or (ii) the cases that are related. This issue should be clarified – there is a need of clarity in which situations the courts are obliged to exchange information about pending court proceedings.

- Also the relationship between Art. 76a and provisions of Regulation No 1215/2012 is not clear. Should Art. 76a be considered as lex specialis in relation to provisions of Regulation No 1215/2012 and to the extent not covered by the draft regulation the provisions of Regulation No 1215/2012 shall apply (i.e. the provisions contained in Section 9 of Regulation No 1215/2012)? If so, is Art. 76a of the draft Regulation equivalent to Art. 29 of Regulation 1215/2012, which refers to proceedings involving the same cause of action, or is it equivalent to Art. 30 of the Regulation 1215/2012, which refers to the related actions?

Art. 77 - Right to compensation and liability

- In **par. 3** Poland proposes to replace "***may***" with "***shall***" which will allow to clarify the exclusion of liability of data controllers and data processors ("*The controller or the processor* ~~***may***~~ ***shall*** *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"*).

art. 79 - General conditions for imposing administrative fines

- **Par. 2a -** The conditions for imposing a fine or other measure, which are referred to in Art. 79 should in the future be clarified in the guidelines of the European Data Protection Board. Otherwise, there is a possibility of different interpretations of these provisions by national authorities and a forum shopping. Poland asks for deletion from footnote 143.

- Moreover, in par. 2a, the aggravating circumstances should be better distinguished from mitigating circumstances (for example in relation to adherence to codes of conduct or certification mechanisms which can be interpreted in both manner – as aggravating or mitigating factors).

art. 79a - Administrative fines

- In Poland's view this provision should be the most simple and clear. We need uniform application of administrative fines in the European Union.

- Poland wants **par. 3a** to be maintained – it clears doubts the controllers and processors might have in the case of accumulation of different violations, which is a good solution.

art. 79b - Penalties

According to Poland, criminal liability, which is the subject of this article, is within the competence of Member States, and should not be harmonised in the EU. Therefore, we preferred the previous wording of this provision, without "***For infringements of the provisions of this Regulation not listed in Article 79a***" should be deleted which will make the wording of this article more precise.

PORTUGAL

I. <u>CHAPTER III</u>

Delegations are asked to indicate whether they prefer to keep a fixed deadline and if so whether the one month suggested is a reasonable period or whether it should be extended or whether it is enough that the controller provides the information without undue delay.

We believe one month to be a reasonable period, therefore would like to keep the draft as it is in that respect.

As regards paragraph 4, delegations are asked to indicate whether they prefer the current wording or if they would like to replace 'manifestly unfounded' by 'abusive'.

We would prefer to keep "manifestly unfounded". We believe this concept to be more precise. In fact to "manifestly unfounded" would correspond "manifestly abusive"?

Delegations are asked to indicate whether they would like to add 'where appropriate/practicable' in the first paragraph or whether they do not think that is necessary. As regards paragraph 1(b) delegations are asked to indicate whether a reference to compatible further processing should be added.

We think not to be acceptable to add "where appropriate / practicable" for the same reasons pointed out by the Presidency. Lower the level of protection already guaranteed by Directive 95/46/EC is unacceptable.

We believe not to be necessary or desirable to add the reference to compatible further processing.

<u>Information to be provided where the data have not been obtained from the data subject (Article 14a)</u>

Paragraph 4 sets out the exceptions to the obligation to provide information. At the DAPIX meeting some delegations asked to delete the last two points (d) and (e) from the list.

Delegations are asked to indicate whether they support the deletion of points (d) and (e) from the list of exceptions.

We prefer to keep the present draft.

The right to be forgotten and erasure (Article 17)

Delegations are asked to indicate whether they prefer to keep the reference to the right to be forgotten or whether they do like the European Parliament approach to delete it.

Without prejudice to the future trialogue with the European Parliament, we believe that the E.U. Parliament approach deserves consideration.

To make effective the so called right to be forgotten involves to stop further spreading of someone's personal data, unless a relevant public or third party interest, protected by law, does not allow it, within the framework of a Member State or Union jurisdiction.

This however poses some practical concerns. In fact, is there really a possible, and insurable, right to be forgotten within the Internet framework? How about the personal data already spread, namely to other national jurisdictions or already legally downloaded, namely by private persons?

It is to be considered that what we may have is just really a realistic right to effectively obtain the erasure of one's personal data within the appropriate jurisdictions and for the moment the respective spread becomes illegal unless a relevant public or third party interest, protected by law, does not allow it, within the framework of a Member State or Union jurisdiction.

As regards the French suggestion, delegations are asked to indicate whether they can support such an addition.

We do not see the need to add the draft proposed by France.

We share without restrictions the concern to protect minors.

However we believe that the consent given by parents or other legal responsible and, within that framework, the respect for the rights of good faith third parties have to be considered even considering that they do not generate "absolute" rights.

This goes without prejudice to the processing of minors personal data within, for instance, the framework of the public education system or the public health system, regarding to witch being forgotten would hardly be conceivable.

The right to be forgotten (Article 17) dispute settlement

Delegations are requested to indicate whether they see the need for a specific dispute settlement for search engines in addition to the rights to lodge a complaint in Article 73 and 75.

We do not see the need to introduce such dispute settlement in the Regulation because we believe that the intervention, at national level, in their specific domains, of DPAs, telecommunication authorities and consumer protection authorities should be sufficient to resolve such dispute.

However we do not oppose that Member States be given the freedom to create autonomous authorities or entities to deal with such disputes, but with believe this should be done without prejudice to the competencies of DPAs.

Data portability (Article 18)

In light of the above, delegations are asked to indicate whether they see/understand the right to data portability as only a right to obtain a copy in a machine-readable format or whether it should also include an obligation for the controller to transmit the data to another controller or third party.

In our opinion the obligation created by the Regulation to guarantee data portability should be limited to the right to obtain a copy in a machine-readable format.

The creation of an obligation for the previous controller to transmit the data to another controller or third party may result from a contractual disposition or specific legal injunction and may have costs.

This should be without prejudice to the data subject right to further use the data by transmitting it to another controller.

Delegations are asked to indicate whether they want to add that this right should not apply to processing when carried out by public authorities or bodies.

Consideration must be given to the possibility of transmission of personal data within the civil law framework of public sector obligations, as well as in the public law framework if provided by law.

If this is not acceptable to all Member States, then the Regulation must allow Member States to enact law for the purposes referred in the previous paragraph.

The right to object (Article 19)

Delegations are asked to confirm if they want to keep the current text without a reference to point (e) of Article 6(1).

We would prefer to revert back to the Commission's proposal. We should not restrict rights already guaranteed by the 1995 Directive.

Delegations are also invited to indicate if they can accept the FR suggestion for a particular point on processing for archiving purposes in the public interest, or historical, statistical or scientific purposes.

The French proposal deserves a positive view. However we ask the Presidency to please take note of a scrutiny reservation regarding the draft being proposed.

Profiling (Article 20)

Delegations are invited to indicate in the first place whether they want to regulate profiling as such or decisions based on automated processing. Delegations are also asked to indicate whether they think that the text or parts of the text adopted by the European Parliament in its report could serve as inspiration for the Council position.

We want to regulate profiling and decisions based on automatic processing. Regarding the positions of the EU Parliament, we believe that it should be left to the trialogue with the EU Parliament. That does not mean we reject them, just that it is may be too soon to express a clear acceptance now.

Delegations are invited to indicate if they see the need to maintain these definitions and if so if the current wording is acceptable.

We support maintaining the current definitions.

II. CHAPTER VIII

Right to lodge a complaint with a supervisory authority and Right to an effective judicial remedy against a supervisory authority (Articles 74 and 75)

Representation of data subjects (Article 76)

Delegations are asked to indicate if they would like to allow such possibilities.

We fully agree with the existence of an effective judicial remedy against supervisory authorities as well as against controllers and processors, without prejudice to the competences of the data protection authorities in what controllers and processors are concerned.

In what the intervention of organisations and associations are concerned it is only acceptable within the framework of the Portuguese law that they go to Court to seek the protection and the respect of their associate's interests.

It is possible that associates, in some associations, namely Trade Unions, benefit from legal counsel and from legal representation by a lawyer paid by the association in question, but it will be the lawyer that will be representing the associate in question.

We propose that article 76 be redrafted in order to refer to the internal law of Member States or be deleted, on the same ground.

Right to compensation and liability (Article 77)

Delegations are invited to indicate if they think that the controller and processor should be jointly responsible or if the data subject should in the first instance address the controller.

The existence of a processor and its choice is a responsibility of the controller. Therefore we favour the option that in principle the controller should be addressed first. If, however, the facts show that the processor acted regarding the personal data entrusted to him in a way contrary to the instructions of the controller, or strange to the contractual relationship established with the controller, the possibility of having them being separately or jointly found responsible is not to be disregarded.

We suggest that, without prejudice to the applicable "acquis communataire", and some desirable uniformity of procedures, Member States keep their own civil and procedural law rules regarding these matters.

Penalties (Article 79b)

Delegations are asked to indicate if they agree with the above wording in the Article and the recital.

We agree with the texts proposed by the Presidency.

FINLAND

WRITTEN COMMENTS AND PROPOSALS ON Chapters III and VIII

Article 17, Right to be forgotten

3. Paragraphs 1 and 2a shall not apply to the extent that (…) processing of the personal data is necessary:

a. for exercising the right of freedom of expression in accordance with Article 80;
b. for compliance with a legal obligation **which requires processing of personal data** ~~*to process the personal data*~~ *by Union or Member State law to which the controller is subject* or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c. for reasons of public interest in the area of public health in accordance with Article **9(2)(g)(h) and (hb) as well as Article 9(4)**;
d. for archiving purposes in the public interest or for *scientific, statistical* **and** historical (…) purposes in accordance with **Article 83**;
e. (…)
f. (…)
g. for the establishment, exercise or defence of legal claims.

Justification: Legislation quite rarely contains obligations to process personal data. Instead there are often obligations which require processing of personal data. An alternative approach would be to align Art. 17(3)(b) with the wording of Article 6(1)(c).

Article 74, Right to an effective judicial remedy against a supervisory authority

Article 74 ***Right to an effective judicial remedy against a supervisory authority***

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~~. (...). **addressed to them or which is of direct and individual concern to them.**

Justification; current formulation “concerning them” is too wide. It should be clarified who are “concerned” in the meaning of Art. 74(1). The drafting proposal is based on Article 263(4) TFEU.

Article 79, General conditions for imposing administrative fines

Article 79 ***General conditions for imposing administrative ~~fines~~ sanctions***

Justification: This Article should apply more generally when assessing the consequences of infringements and also take properly into account the possibility to issue reprimands.

~~1. Each supervisory authority [competent in accordance with Article 51] shall be empowered to impose administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in Article 79a. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in Article 53.~~

Justification: This para is superfluous with Article 53(1b)(g). It has no added value in this Article. Deleting this para would make the text more simple and easier to read.

~~2. Administrative fines imposed pursuant to Article 79a shall in each individual case be effective, proportionate and dissuasive.~~

Justification: This para is not necessary, because para 2a gives more concrete content for “effective, proportionate and dissuasive”. In any case, it could be removed to after para 2a.

2a. When deciding whether to impose an administrative fine in addition to, or instead of, measures referred to in points (a) to (f) of paragraph 1b of Article 53 and deciding on the amount of the administrative fine in each individual case due regard shall be ~~had~~ **given** to the following:

(a) the nature, gravity and duration of the infringement having regard to the nature scope or purpose of the processing concerned;
(b) the intentional or negligent character of the infringement,
(c) **the gravity of infringement having regard** the number of data subjects affected ~~by the infringement~~ and the level of damage suffered by them;

Justification: The weight should rather be on the act itself, not on the consequences of the act as the consequences might not be predictable.

(d) action taken by the controller or processor to mitigate the damage suffered by data subjects;
(e) the degree of responsibility of the controller or processor having regard to technical and organisational measures implemented by them pursuant to Articles 23 and 30;
(f) any previous infringements by the controller or processor;

~~[(g) any financial benefits gained, or losses avoided, directly or indirectly from the infringement;]~~

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i) **in case** measures referred to in point (b) and (c) of paragraph 1 and points (a), **(ca),** (d), (e) and (f) of paragraph 1b of Article 53, **have previously been** ordered against the controller or processor concerned with regard to the same subject-matter, *compliance with* ***these measures*** ;

Justification: (ca) should be added to point (i).

(j) adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39;
(k) (…);
(l) (…);
(m) any other aggravating or mitigating factor applicable to the circumstances of the case.

2b. (…).

3. (…)
3a. (…)

2 - 3(aa) Administrative ~~fines imposed pursuant to Article 79a~~ sanctions shall in each individual case be effective, proportionate and dissuasive. In a case of a minor infringement [or if the fines imposed would constitute an unreasonable burden to a natural person], a reprimand referred to in point (b) of paragraph 1b of article 53 shall be issued instead of fines. Due regard shall however be given to the intentional character of the infringement, to the previous infringements or any other factor referred to in paragraph 2a.

Justification: If this para is kept, it should rather be placed here with the proposed amendments. This Article should apply more generally when assessing the consequences of infringements and also take properly into account the possibility to issue reprimands.

3b. Each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

4. The *exercise by the supervisory authority* [competent in accordance with Article 51] of its powers under this Article shall be subject to appropriate procedural safeguards in conformity with Union law and Member State law, including effective judicial remedy and due process.

Article 79(a), Administrative fines

Article 79a

Administrative fines

1. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR, or in case of an undertaking […] % of its total worldwide annual turnover of the preceding financial year, on a controller who, intentionally ~~or negligently~~:

(a) does not respond within the period referred to in Article 12(2) to requests of the data subject;
(b) charges a fee in violation of the first sentence of paragraph 4 of Article 12.

2. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR, or in case of an undertaking […]% of its total worldwide annual (…) turnover of the preceding financial year, on a controller or processor who, intentionally ~~or negligently~~:

(a) does not provide the information, or (…) provides incomplete information, or does not provide the information timely or in a ~~sufficiently~~ transparent manner, to the data subject pursuant to Articles 12(3),14 and 14a;
(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not comply with the rights and obligations pursuant to Articles 17, 17a, 17b, 18 or 19;
(c) (…);
(d) (…);
(e) does not ~~or not sufficiently~~ determine the respective responsibilities with joint controllers pursuant to Article 24; (f) does not ~~or not sufficiently~~ maintain the documentation pursuant to Article 28 and Article 31(4).
(g) (…);

3. The supervisory authority [competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR or, in case of an undertaking, […] % of its total worldwide annual turnover of the preceding financial year, on a controller or processor who, intentionally ~~or negligently~~:

(a) processes personal data without a (…) legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7, 8 and 9;
(b) (…);
(c) (…);
(d) does not comply with the conditions in relation to (…) profiling pursuant to Article 20;
(e) does not (…) implement appropriate measures or is not able to demonstrate compliance pursuant to Articles 22 (…) and 30;
(f) does not designate a representative in violation of Article 25;
(g) processes or instructs the processing of personal data in violation of (…) Articles 26;
(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject in violation of Articles 31 and 32;
(i) does not carry out a data protection impact assessment in violation of Article 33 or processes personal data without prior consultation of the supervisory authority in violation of Article 34(1);
(j) (…);
(k) misuses a data protection seal or mark in the meaning of Article 39 or does not comply with the conditions and procedures laid down in Articles 38a and 39a;

(l) carries out or instructs a data transfer to a recipient in a third country or an international organisation in violation of Articles 40 to 44;
(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1) or does not provide access in violation of Article 53(2).
(n) (…)
(o) (…).

[3a. If a controller or processor intentionally ~~or negligently~~ violates several provisions of this Regulation listed in paragraphs 1, 2 or 3, the total amount of the fine may not exceed the amount specified for the gravest violation.]

4. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of adjusting the maximum amounts of the administrative fines referred to in paragraphs 1, 2 and 3 to monetary developments, taking into account the criteria referred to in paragraph 2a of Article 79.]

UNITED KINGDOM

UK proposed textual amendment – Article 17, Paragraph 2a

Issue:

Paragraph 2a of Article 17 ("the right to be forgotten and to erasure") obliges controllers "to take reasonable steps, including technical measures, to inform known controllers which are processing the data, that a data subject requests them to erase any links to, or copy or replication of that personal data".

Solution:

In order to recognise the inherent difficulty in tracing information once it has been disseminated in the digital age and to make the obligation on data controllers proportionate and workable in practice, the UK considers that the Council should say more in the text about what constitutes a "known controller". The benefit of this approach would be to:

- provide greater legal certainty for data controllers in terms of their obligations in relation to other controllers to whom the data has been disclosed; and

- provide greater clarity for data subjects about their actual rights under this provision.

Proposed textual amendments:

In order to provide this clarity for data subjects and data controllers alike, the UK proposes that the Council includes within the operative text of Article 17 the following wording:

"A "known controller" is a controller whose identity was known to the controller that made the personal data public at the time it was made public and to whom the data was intentionally disclosed by that controller."

For the purposes of absolute clarity, this should be supported by an accompanying recital that states:

A "known controller" is a controller: "whose identity was known to the controller that made the personal data public at the time it was made public. It should also only extend to controllers which fall into that category who were deliberately and intentionally provided with the data by the controller which made the data public."

General comment on Article 17 (and associated recitals)

On a separate issue raised by the Presidency in their paper of the 27 March (7526/15), The UK would like to reaffirm its position that the "right to be forgotten" and all other references to this wording in the draft text should be deleted. We agree with the premise put forward by Spain in their position paper, that the right to be forgotten" suggests an unfettered right for data subjects to have their personal data deleted that does not exists in practice. Rights should be deliverable in practice, to do otherwise only serves to undermine data protection rules.

Recital 53a

Recital 53a seeks to set out how data controllers should approach the balancing act between the privacy rights of individuals and the legitimate interests of internet users in accessing the personal data in question. It states that:

"Inasmuch as the removal of links from the list of internet search results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst the data subject's rights protected by those articles should override, as a general rule, the interest of internet users, that balance may in specific cases depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having access to that information, an interest which may vary, in particular, according to the role played by the data subject in public life".

This recital therefore places greater weight, as a general rule, on the privacy rights of individuals over the legitimate interests of internet users in having access to that information. This is a clear attempt to carry over *some* of what the CJEU said in *Google Spain*. It is common ground in the UKs view that there is no legal obligation to replicate any part of that judgement when deciding on the content of the proposed Article 17.

It is wrong in principle, and potentially dangerous in practice, to assume that the findings of the Court in *Google Spain* will apply without modification in respect of the proposed Article 17 right. Those findings were made in the specific context of existing rights in the current Directive. There are significant differences between those rights and proposed Article 17.

Further, the UK considers that this is not the right place to decide where the balance between privacy rights on one hand and the rights of internet users on the other lies. The question of how competing rights are to be balanced in individual cases for the purposes of ensuring Charter compatibility is properly a matter for the CJEU, if and when the matter is referred to it for consideration. Attempting to interpret this balancing exercise in the recitals, and the associated question of compatibility with the data subject's fundamental rights under Article 7 and 8 of the Charter of fundamental rights only serves to pre-empt any decision of the CJEU. Not only is that inappropriate, it is also potentially deeply unhelpful.

For this reason, the UK considers that recital 53a should be deleted.

Article 77

Introduction

During the interesting and illuminating discussion of Article 77 in the DAPIX of 31st March, it was apparent that different definitions and concepts of joint and several liability across Member States led to a certain amount of confusion on the matter.

This is why simplicity is vital. That is the bedrock of the position put forward by the UK at that meeting and summarised here. A system under which "liability follows the fault" can be understood across all Member States by data subjects, controllers, and processors alike without recourse to concepts of joint and several liability. Our view is that controllers or processors should only be liable for breaching an obligation that applies to them under the GDPR, and for the damage this breach has caused.

In light of this and the analysis that follows, we hope that Member States will look favourably on our proposal to include the following drafting, as first proposed verbally at the last DAPIX:

77.2 ***Where more than one controller or processor or a controller and processor are involved in the processing that gives rise to the damage, each controller or processor shall be liable only for the damage caused by its actions and which arises from breach of an obligation imposed on it by the Regulation. This is without prejudice to recourse claims between controllers and/or processors.***

Not only is the substance of this proposal sensible and fair, it reflects the current position under the 1995 Directive, which we understand to work well. Indeed, as our comments below make clear, it also reflects a central assumption underlying the drafting of Article 77 itself in the current text: that a party shall not be liable for things it has not done wrong (Article 77.3). To that extent, as well as eliminating the damaging lack of redress described below, adopting the UK's proposal will eliminate an important internal inconsistency in the current text between Article 77.2 and Article 77.3.

The UK's objective in putting forward this proposal is to give legal certainty and justice for data subjects, data controllers and data processors. It does by avoiding the very serious problems with the joint/several liability proposal, as set out below. Most serious of these is that we believe the current text will not add value to data subjects. Contrary to the claims of its supporters, it may even undermine the protection of data subject's personal data, of which the right to appropriate and effective compensation is such an important part.

Problems with Joint and Several Liability for Data Subjects and Businesses

Joint and several liability poses several disadvantages. Firstly, it appears to have limited benefits for the data subject in question. We understand that the Commission's priority is to ensure that the data subject receives compensation as soon as possible. However, this is not guaranteed – and may even be undermined – by the text.

Effective compensation is about more than speed. Central to the problems inherent in the current drafting of Article 77 is a misconceived assumption that enabling a data subject to bring proceedings against as wide a range of parties as possible will result in more effective redress.

One apparent advantage of joint and several liability, emphasised by some delegations at the last DAPIX, is that a data subject may take any of the controllers or processors "involved in the processing" to court without needing any indication of who could be at fault. While this may appear quicker in the short term, it works against a successful outcome by providing false reassurance about the likelihood of receiving compensation. If the data subject has chosen a controller or processor without focussing on their guilt, they run the risk of the controller/processor being able to demonstrate successfully in court that they are not at fault for the damage in question. If the controller/processor succeeds, they cannot be held liable, jointly or severally, as Article 77.3 makes very clear. The data subject would leave court empty-handed, having wasted time, money, and public resources.

Secondly, to compound the problem, the culpable party to the breach may avoid any legal action at all should the data subject in question not have the financial means to pursue a fresh claim for compensation. This is where some delegations' desire for a quick route to compensation for the person in question risks frustrating the very aim it seeks to achieve. For that reason, it should not be the objective or priority of this Article. The priority should be protecting the rights of all data subjects who may still be having their rights violated by the party who is truly at fault. Encouraging or enabling pursuit of a faultless party at random will not stop the party at fault from carrying on breaching the GDPR and causing damage to other individuals. Furthermore, it provides neither justice for the data subject or the controller or processor that was incorrectly pursued.

Thirdly, joint and several liability could create certain perverse incentives leading to situations where the rights of data subjects and the security of their personal data are undermined. Joint and several liability spreads out the risk regardless of fault. The more parties involved, the less the risk may be for each party. The risk will also be less for those processors who are unknown to the data subject. This acts as an incentive for parties to cut corners on security or other obligations, knowing that they are less likely to be pursued and held accountable for their actions.

This problem should not be understated. More and more data is being processed in the Cloud where a long chain of multiple processors is the norm. The distance between the end user or data subject and the processor at the end of the chain offering Infrastructure as a Service (IaaS) is considerable. Many processors in the Cloud also face even less risk due to outright excluding liability in their contracts even for loss of data, or else limiting liability to a capped token amount or service credits.

Finally, joint and several liability may not only harm data subjects, it also harms the parties pursued who are not at fault, particularly SMEs. Reputational damage is not easily recovered. Court cases are a matter of public record. Guilt by association will be impossible to avoid: the mere news that a controller or processor is being pursued for damages after a breach risks obliterating the trust that its customers have in it, as well as deterring potential customers.

Even a party that successfully defends itself through A77.3 will suffer damage to its reputation. Recovering costs through a contract will not solve this: the recovering party will receive little or no publicity, and contractual claims will likely not be resolved until some time after the court case concludes. Furthermore, it may be too late if the initial adverse publicity means that the organization no longer exists, having lost so many customers at the time the claim was brought, or having incurred such high legal costs in defending an action, that it has gone out of business. The potential effects of such a liability may also act as an entry barrier, discouraging new micro or SME entrants to the processing market. This in turn undermines wider goals of tackling online barriers in the Digital Single Market and unlocking the potential of the Cloud sector in Europe.

Solution – simple fault-based liability

The last section has listed the various disadvantages posed by joint and several liability: it does not necessarily lead to quick compensation for the data subject; the parties truly at fault may continue without being held to account; risk-sharing may incentivize further risky practices; blameless parties may suffer reputational damage that will have negative consequences for their business and the processing market in the EU. In addition, as we have seen, the concept is overly complex and varies across Member States.

These points reflect essential objectives or criteria for the model of liability that we choose. The model must be simple and understandable. It must lead to effective compensation for the data subject. It must be targeted at ending damage suffered potentially by data subjects beyond the individual in question. It must avoid causing unnecessary reputational damage to innocent parties.

It must add value for individuals and businesses. A system of liability that "follows the fault" can attain these objectives. With a system that focuses on fault, effective compensation is more likely for data subjects. Parties who are at fault will be held accountable and thus will be encouraged to fulfil their obligations. Parties who are not at fault will suffer less damage to their reputation. Last but not least, a fault-based system offers simplicity. It is good for individuals and good for businesses.