



Council of the
European Union

Brussels, 31 July 2014
(OR. en)

12274/14

Interinstitutional File:
2012/0011 (COD)

LIMITE

DATAPROTECT 108
JAI 626
MI 575
DRS 103
DAPIX 108
FREMP 147
COMIX 396
CODEC 1672

NOTE

From: General Secretariat of the Council
To: Delegations
Subject: Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
- The right to be forgotten

Delegations will find below comments regarding the right to be forgotten.

TABLE OF CONTENT

BELGIUM	3
ESTONIA	5
SPAIN	14
FRANCE	15
CROATIA	18
LUXEMBOURG	20
HUNGARY	21
AUSTRIA	22
POLAND	24
ROMANIA	27
SLOVAK REPUBLIC	28

BELGIUM

BE wants to draw your attention on the fact that the CJEU case concerned only one typology of Internet intermediaries: the search engines. The article 17 applies to all the controllers independently of their nature. We should then be cautious when adding some obligations or precisions in the article 17 that could potentially be too much tailored for specific intermediaries. The regulation should remain horizontal.

1. Delegations are invited to reconsider the introduction of the words “relating to them” which appears to better clarify the scope of the exercise of rights by the data subject.

BE is not in favour of the introduction of the words “relating to them”.

2. The Presidency therefore invites delegations to express themselves as to whether the wording of paragraphs (a) and (d) of Article 17(1) should be amended, for example by adding ‘by that controller’.

BE has a scrutiny reservation on that point. The distinction between the preliminary controller and the second controller needs to be further assessed.

3. Delegations are invited:

- to confirm that it shall be for Member States to reconcile the right to the protection of personal data with the right to freedom of expression

BE isn't sure to understand this question. The room for manoeuvre for MS concerning the right to freedom of expression is in the treaty. There is no harmonization on that topic. The balance between those two rights is different within the MS.

But BE thinks that the relation between article 17 and article 80 should be more elaborate. Indeed, the court doesn't only mention the right to freedom of expression but also the right to receive and impart information. The right to be forgotten should therefore be balanced with all applicable fundamental rights.

A question could be to know how a kind of harmonisation could be founded. The Regulation could delegate to the Commission, to the DPA's or to the EDPB the creation of common procedural guidance for MS and for the controllers.

- To confirm, in the light of previous discussions and the Google judgment, that the data subject has the choice to exercise their right to be forgotten and to erasure against any of the controllers involved, without regard to an order of controllers according to which these rights have to be exercised.

There is no question of order between controllers but in practice, it may be interesting for the second controller to know the opinion of the controller which has published the information.

It isn't always easy for a search engine to make the correct balance between the rights concerned.

4. Delegations are invited to indicate whether they see a need to maintain paragraph 2a of Article 17.

BE thinks that there is a need to maintain this §2a. At the same time, it's also needed to better define what information should be given and to whom. BE has proposed to add "known" controller in order to add legal certainty.

ESTONIA

I. The right to be forgotten (article 17)

In the previous working party, we discussed the right to be forgotten in the light of the Google judgment. Furthermore, the presidency has asked us some questions regarding the possible way forward with article 17 (document No. 11289/14). We would like to hereby take the opportunity and send our answers in writing:

(1) The scope of the right:

It has been asked, if there is a need to introduce the words “*relating to them*” in article 17(1) for the purpose of clarifying the scope of the exercise of rights by data subject (*question in point 8*). As mentioned in the working party, we believe that the introduction of these words is not essential. On one hand, indeed article 17(1) mentions only personal data, which is any information relating to an identified or identifiable natural person according to article 4(1). We understand that the wording of article 17(1) “*the data subject shall have the right to obtain the erasure of personal data*” might imply that you can use the right set out in article 17 towards any personal data not only the data related to yourself. However, on the other hand, recital 53 clarifies clearly that the erasure can be sought for the personal data related to them using the notions “*personal data concerning them*” and “*their personal data*”. Therefore, it can be interpreted, that the right can be used only regarding my own personal data. However, for legal clarity it might be useful to also include it to the main text. To sum up, we believe that it is not necessary to include the words “*relating to them*”. However, it might be useful due to the legal clarity. Therefore, we support the Presidency’s proposal to clarify that the right can be used only towards the personal data concerning that person. In the latter, we suggest (as also pointed out by the Irish delegation) to review also the wording of other rights as well as recitals explaining the rights to achieve legal consistency (e.g. recital 53, which explains article 17, uses notions “*personal data concerning them*”; and article 17a(1) does not have the previously mentioned words either).

(2) The grounds on which this right can be exercised:

The Presidency has invited us to discuss, if there is a need to amend article 17(1)(a) and (d) in light of the Google judgment as to the controller's obligation to analyse the necessity and the lawfulness of processing (e.g. by adding the words "*by that controller*") (*question in point 14*).

We believe, similarly to the previous question, that there is *per se* no need to add the previously mentioned words. Namely, as mentioned also by other delegations in the work party, article 17 does not differentiate or make a distinction between the so called initial controller and second controller. Therefore, the current text sets out an obligation to exercise the necessity/lawfulness test for all controllers. Furthermore, the controller can only analyse the processing activity of themselves not a different controller. Therefore, in our opinion, the text already covers the fact that all controllers should analyse their own processing activity.

To sum up, we believe that it is not essential to include new words to the text, but once again we are also not against it and can support the Presidency's proposal, if there is a need.

(3) The need to balance the right to protection of personal data with the freedom of expression and the interest to access to information:

We have been invited to confirm (a) that the Member States have to reconcile the right to the protection of personal data with the right of freedom of expression; and (b) that the data subject has the choice to turn to any of the controllers involved regarding the right to be forgotten and erasure (*question in point 24*).

(a) We agree that there are no absolute rights and we do have to find a way for different fundamental and constitutional rights to exist together. Furthermore, we have to find a balance in several different situations and circumstances. However, we believe that we should leave it to the Member States to reconcile the right of protection of personal data with the right of freedom of expression. Namely, the right can be balanced via specific laws (i.e. journalism) and also in administrative proceedings by the DPA while applying and interpreting the data protection regulations in practice (taking into account the EU and national court practice in the matter).

Therefore it would not be reasonable to regulate the notion and rules of reconciliation in detail in the data protection regulation as it falls outside of the scope and competence of data protection. Furthermore, the reconciliation might be often part of a different law field, which has its own principles (e.g. civil law, journalism etc.) and the reconciliation might have a specific basis considering the specific law.

To sum up, we confirm that the reconciliation of the two previously mentioned rights has to stay up to the Member States.

(b) We also believe, as some other delegations, that the court does not set an order between the initial and second controller in Google judgement. We believe that these are different processing situations, which have to be analysed separately. There might be indeed cases, whereas both situations are at the same time illegal or at the same time legal, but it depends on different circumstances. Furthermore, according to the judgement, we cannot assume in case of lawfulness of the initial processing that the second processing is also legal. Therefore, it would be more reasonable and it would ensure a higher protection for the data subject, if he or she could choose any of the controller to turn to.

To sum up, we agree that the data subject should have the right to choose any of the controllers involved to exercise their right to be forgotten and erasure as well as no order between the initial and second controller should be created.

- (4) The need to impose an effort obligation on initial controller to inform secondary controller to erasure of data:

We have been invited to indicate, if we see a need to maintain paragraph 2a of article 17 or not (*question in point 28*).

Following the discussions in the working party, we would like to indicate our support to redraft paragraph 2a of article 17. Namely, we could keep it only as an obligation, if the data subject requests it. We believe that in this way we would find a balance between the protection of the rights of the data subject and the administrative burden of the controllers. We think that even in the light of the Google judgment, the obligation to inform other (known) controllers, which are processing the data, about the fact of erasure, might be beneficial for the data subject. According to the judgement, in a particular case, the initial and second controller had different outcome of the lawfulness. However, the court did not rule out, that in some cases and circumstances the data subject might have a right to ask for erasure from both controllers. If the data subject would like to erase it from everywhere and there is a legal ground for that, then paragraph 2a has an added value as the initial controller might have a higher possibility with reasonable steps to inform the other controllers. We believe that the purpose of this paragraph could be to notify other controllers to exercise the necessity and lawfulness test in cases, where the data subject would like to erase it from everywhere.

To sum up, we do believe that paragraph 2a of article 17 might still have an added value, even considering the Google judgement. However, considering the discussions in the working party, we believe that the notification obligation has to be limited to cases, where the data subject explicitly requests it.

II. Article 33(2)(e) in close connection with articles 33(2a) and (2b) as well as articles 52(1)(fa) and 57(2)(c)

a. Separation of powers, including the power to adopt legislative acts

Firstly, we would like to briefly explain the legal system of Estonia. We understand that it might not be necessary as the misunderstanding of our reservation might have been caused by the translation and/or the shortness of our intervention(s) at the DAPIX meeting. However, to avoid any further misunderstandings, we will shortly describe the separation of powers.

Namely one of the main principle in our constitutional law is the separation of powers (known in EU as the institutional balance) (Estonian constitution § 4). We believe it is not an unknown principle also to other European countries. The powers are divided as follows: legislative (Parliament), executive (Government) and judicial power (Courts).

The legislative power includes the power to adopt legislative acts as well as delegate some of the legislative power to the Government. However, this is restricted by the Constitution, that legislative powers are only attributed to the specific Government institutions such as ministers only based on certain delegation norm adopted by the Parliament (Estonian constitution § 3, § 59, § 86ff). Administrative authorities and government bodies (such as DPAs) are prevented from using the general legislative powers.

Therefore, it will be against our constitution to give the legislative power to the DPA. We believe that this principle does not go against the decisions of the European Court of Justice, whereas the scope of the independence of the DPAs is being explained and stressed. Namely, it points out that *“the guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim.”* Therefore they should be independent and free from external influence regarding their activities (i.e. in particular the supervision and decision-making power), but the independency does not include the legislative drafting power.¹

To sum up, our constitutional problem originates from the mere fact, that the supervisory authorities do not have the competence (according to our constitution) to adopt legislative acts (i.e. legislative power). However, this might be a general principle in several member states, which means that the difference of opinion might arise actually from the notions *“legislative act”* as well as *“administrative act”* and the content of article 33(2)(e) and (2a).

¹ European Court of Justice, Case No. C-518/07 p 19, p 25 and 30 (and others); (Furthermore: Cases No. C-614/10 and C-288/12).

b. Legislative act vs administrative act

In general, we think that the power given to the DPAs in article 33(2a), in close connection with 33(2)(e), is a legislative power according to our legal system. Following clarifications explain our statement.

Firstly, article 33(2) provides the controller's obligation to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data, where the processing, taking into account the nature, scope or purposes of the processing, is likely to present specific/high²risks for the rights and freedoms of data subjects. Article 33(2) names the operations, which present specific/high risks, referred to in paragraph 1.

Furthermore, article 33(2)(e) specifically provides that the competent supervisory authority can consider that other operations, than specified in art 33(2)(a) – (d), present specific risks for the rights and freedoms of data subjects. This article on its own does not cause any problems as the DPAs have the right to interpret the law and in certain cases in an administrative proceeding decide that this particular operation is likely to present specific/high risks and the assessment of the impact has to be carried out.

However, article 33(2a) stipulates that the supervisory authority shall establish and make public a list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. Considering the content and the scope of addressees of this list, it is not a mere administrative act of the DPA but a legislative act.

There are three types of legislation: primary legislation (laws of general nature adopted by the Parliament), secondary legislation (ministerial regulations of general nature adopted in accordance with specific delegation norm in the primary law and specifying the primary law) and administrative acts (decisions by the public authorities made while exercising their powers and addressed to an identified number of addressees).

² For the purposes of clarity we have used throughout the text both words “*specific*” and “*high*” as it has been recently changed for article 33(1) and (2) but not for 33(2)(e).

In case of administrative acts, it is possible to distinguish an individual act (an order made to a particular addressee and regulating a particular situation) and general act / general order (an order addressed to persons determined on the basis of general characteristics and regulating an individual case). The differentiation of general orders (possible to issue by the DPA) and legislative acts (possible to adopt only by Parliament or in certain cases by the Government) is an important one and includes several elements. In the current case, we will explain two crucial elements of general orders.

- (a) Persons determined on the basis of general characteristics: We do not see the general characteristics, which allow us to determine the persons to whom this decision of the DPA will be addressed/directed. This will apply technically to all controllers, who are planning to engage into processing operations considered to be presenting specific/high risks for the rights and freedoms of data subjects.
- (b) Individual case: Individual case is a particular situation, which is identifiable with a specific vital fact or behaviour. We believe that the list will apply to undefined number of cases, not to an individual case.

To sum up, it is not possible to determine the addressees on the basis of general characteristics nor does this list regulate an individual case. Hence, according to Estonian legal system, the list will be considered as an abstract legal provision to regulate undefined number of cases as well as persons. This means that it is a general and abstract regulation, i.e. a legislative act, which cannot be issued by the DPA, who does not have any legislative power and this power cannot be given to them due to the principle of separation of powers.

c. Proposal

Following the previously described reasons and analysis, we have two different alternatives for rephrasing the article 33(2a) and (2b):

1) We would suggest to erase article 33(2a) and (2b) as well as articles 52(1)(fa) and 57(2)(c).
This will leave us with the situation that the competent DPAs can still consider other processing operations likely to present specific risks for the rights and freedoms of data subjects. However, this would and should be a case-by-case decision in the administrative proceeding(s). Furthermore, the administrative practice of the DPA can also be considered as an indication to companies, i.e. if in one administrative proceeding the DPA has considered an activity to cause specific risks, then it is highly likely that it will have to make the same decision in a similar case.
Although, we also believe that article 33(2)(e) might be unnecessary as the same goal would be achieved by adding the words “*in particularly*” or “*for example*” in article 33(2), i.e. leaving the list non-exhaustive and giving the DPAs the possibility to consider other processing operations causing specific/high risks.

2) We would suggest giving the lists named in articles 33(2a) and (2b) an indicative/advisory nature. In this case it would be considered like guidelines or an advisory role/power of the DPA and it would not go against our constitution. Therefore the list will be as an indication to the companies and it is highly likely that the DPA will decide in a specific case with similar processing activities, that it is likely to present specific risks.
Hence our wording proposal for articles 33(2a) and (2b) is following:

*2a. The supervisory authority shall establish and make public an **advisory** list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.*

*2b. Prior to the adoption of the **advisory** list the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where the **advisory** list provided for in paragraph 2a involves processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.*

Furthermore, for legal clarity, we suggest changing the wording also in articles 52(1)(fa) and 57(2)(c):

*52(1)(fa): establish and make **an advisory** list in relation to the requirement for data protection impact assessment pursuant to Article 33(2a);*

*57(2)(c): aims at adopting **an advisory** list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 33(2b); or*

III. Article 34 “Prior consultations”

As mentioned in the working party, we would be in favour of exempting the controllers from the obligation of prior consultations, if they have appointed a DPO. We believe that it would be a good balance between the administrative burden of the controllers as well as the rights and freedoms of the data subject. Therefore, we would kindly ask you to add us to the footnote 103 on page 41 of the document No. 11481/14.

SPAIN

Question 1

Except for the cases in which a person has been formally named as the representative of another, the subjects can only exercise his or her rights regarding data “relating to them”. Therefore, we see no need for including the terms suggested by the Presidency.

Question 2

Again, Spain considers unnecessary to add the words “by that controller” in Article 17.1.a) and d). The ECJ judgment clearly states that the search engines develop data processing operations that are a different from processing operation of the “original controller” of those data. Consequently, the search engine will be responsible for that processing operation, subject to the general principles of data protection and to the possibility for the data subject to exercise its rights. Bearing this in mind, we understand that the wording of paragraphs s) and d) of Article 17.1 already applies to “second controllers”.

Question 3

From our perspective, the most appropriate moment to deal with the issue of pondering the rights of data protection and freedom of expression would be the discussions on Chapter IX (Art. 80). Anyway, the ECJ judgment has not altered the Spanish position related to this matter, so we still generally support Art. 80 as it stands now.

As regards the second question, the Spanish delegation considers that the adequate interpretation of the ECJ judgment blocks the possibility of imposing an “order” for the data subject to exercise its rights against the controllers. As stated above, the judgment clearly states that the search engine activity implies a data processing which is different from the one carried out by the “original processor”. According to the judgment, it should be perfectly possible for the data subject to exercise its rights against the processing operation carried out by search engine before, after or independently from exercising the same or other rights against the original controller for its processing operation.

FRANCE

We thank the Presidency for its working document and for organising talks following the Court's judgment in the Google Spain case (Case C-131/12).

In general, we reiterate that we have always been in favour of introducing the right to be forgotten in the proposal for a Regulation.

In addition, we still maintain that the right to be forgotten and the right to erasure should not apply to **archives**. The derogation under Article 17(3) in the Presidency compromise text is a step in the right direction but coordinating it with Article 83a remains problematic in the light of the current wording of that Article.

Regarding the right to be forgotten, and more specifically the right to delisting established by the ECJ in its judgment of 13 May 2014 in the Google Spain case (Case C-131/12), we are still considering the matter and therefore wish to enter a **general reservation on Article 17**.

Even so, we would like to share our thoughts to help fuel the debate initiated by the Italian Presidency on that right and on the consequences of the Court's judgment. In this regard, **we wish to share seven concerns:**

- Should the proposal for a Regulation specify to whom initial requests to exercise the right to be forgotten must be addressed? If so, should requests be addressed directly to the controller (including search engines, in accordance with the judgment)? To the supervisory authority? To the competent courts? It is worth noting that following the ECJ's judgment, Google received approximately 85 000 delisting requests from across the European Union between mid-May and mid-July, with approximately 1 000 further requests being made every day.

- These questions are directly linked to the issue of determining which courts have territorial jurisdiction, in particular in relation to the one-stop shop mechanism, and, consequently, which law applies.

Indeed, under the one-stop shop mechanism, requests would be examined by the supervisory authority in the place of residence of the persons concerned. However, as the text stands, if the supervisory authority upholds the request of the person concerned, any appeal against that decision by the controller would have to be brought before the courts of the Member State of the one-stop shop. Consequently, those courts would have to implement the right taking into consideration other rights and freedoms guaranteed by their national legislation (in particular the right to privacy and the right to freedom of expression).

- There is also the issue of determining criteria to coordinate the different national laws and different rights and freedoms at stake.

At this point, we feel that national legislation in the area of freedom of expression and privacy should be preserved and should not be covered by a harmonised approach in the proposal for a Regulation on data protection, considering the different approaches – in particular from a cultural point of view – to the matter (it is very much a judicial matter in France). Furthermore, at first sight, the legal basis of the proposal for a Regulation does not seem to allow for harmonisation in this matter.

- If requests were to be made directly to controllers, would it be necessary – and desirable – to establish a further obligation for controllers to facilitate the exercise of the right in question, in particular by making forms available to the persons concerned (similar to those made available by Google immediately after the Court delivered its judgment)? If so, should that obligation apply solely to controllers who make data publicly available?

In any case, at this point, we are basically in favour of limiting the scope of the obligation to inform, provided for under Article 17(2a) and applicable to controllers upholding a request in relation to the right to be forgotten, to the direct recipients of the data.

- What role should the supervisory authorities play in implementing the right to be forgotten? In particular, how can they enforce the right to be forgotten and, in doing so, will they be able to arbitrate between, for example, the right to be forgotten and the right to freedom of expression or freedom of information? Might it be necessary to establish criteria enabling them to coordinate those different rights and freedoms, and if so, what criteria?
- How might the rules on competence sharing to be stipulated in the proposal for a Regulation on data protection tie in with the potential revision of Regulation No 847/2007 of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) (and in particular with the planned extension of its scope to invasions of privacy and infringements on personality rights, including those in the area of libel)?
- In the context of processing delisting requests, as highlighted by the Presidency, should the examination of these requests be linked to the examination of requests for the erasure of "initial" data?

CROATIA

We fully supports the position of the ECJ in accordance with the provisions of Directive 95/46/EC, that Internet search engines represent controllers and that their actions on personal data processing represents personal data processing.

With regard to the question about the scope of the article 17 para 1, and the proposal to consider the possibility of listing the phrase "relating to them" after the words "personal data", we believes that such a change does not represent any substantive change, and that there is no added value, so the text of the article is quite well understood without such an addition. Also, there is a possibility that such an amendment (adding "relating to them") can make certain provisions a bit confusing.

Regarding the question about the right to be forgotten, we believes that regardless of the number of controllers, each of them must collect and process personal data in accordance with the law and based on valid legal grounds. Also, each controller is obliged to process personal data to the minimum extent necessary to achieve lawful purposes, and in this sense we have no objections to the content of art. 17 para 1 a) and d). Furthermore, we believes that the use of the terms "first" and "second" controller can lead to confusion as such terminology is not known in the regulations on the protection of personal data, nor in the judgment Google vs. Spain. The fact of the first controller does not diminish the responsibility of other controllers to process personal data based on valid legal basis.

Regarding the relationship between the right to protection of personal data and the right to freedom of expression and access to information, we consider that the text must take into account the findings of the ECJ to balance between the competing rights and interests. We believes that the solution proposed in the article 80 and 80(a) are good. However, we believes that in art. 80 should clearly highlight the need to balance between the respective rights and to erase the word "reconcile" and replace it with the words "balance between". In fact it would be a clear manner the provisions of the above Articles to the simultaneous obligation to respect the provisions of the relevant law on the protection of personal data and the relevant provisions on freedom of expression, and the balance in accordance with national regulations regarding the possibility of personal information in a particular situation. We also believes that there must be no mixing of different roles of controllers since each of them collects and further processes personal data based on specific legal grounds which may be different, and each of them has to assess whether is it authorized or required to collect and erase personal data of data subjects. Consequently we confirm our view that the MS in accordance with the proposed Art. 80 of the Regulation, has the right through its national laws to determine the balance between the right of protection of personal data and the freedom of expression. With regard to the realization of their rights, data subject shall have the right to freely decide to which controller will lodge a complaint in relation of the right to be forgotten.

We also points out that that the provision of Art. 17 point 2(a) is helpful and advocate for its retention. Firstly, we should consider that it is primarily for information purposes and is not an order for the deletion, and on the other hand should recognize the fact that controller will be in a position to assess whether they have valid grounds for processing of personal data, and if they are not, then can move to the deletion of irrelevant data.

LUXEMBOURG

For Luxembourg, it is fundamental that the proposed Regulation remains technology neutral and applies both online and offline. This should also be the case with the right to erasure and a possible right to be forgotten that needs to be horizontally applicable, irrespective of the type of data processing. This judgment should therefore be seen as an application of the right to erasure in a very specific context, and the co-legislators should be careful before translating its main affirmations into a horizontally applicable Regulation.

As far as the articulation, or balancing, between the right to be forgotten and fundamental rights and freedoms such as freedom of expression or right to information is concerned, this should be evaluated on a case by case basis. National legislation about the ‘other’ fundamental rights (cf Chapter IX) provides the framework for such articulation. National competent authorities should be consulted, if necessary, to clarify situations that may not appear evident for this balancing act.

Concerning the scope of the exercise of rights by the data subject, Luxembourg believes they should be realistic both for the controller and for the data subject: only the personal data relating to the person requesting the deletion should be concerned by this right. Furthermore, the request to erasure/forget needs to aim at specific data and not be formulated in a general way.

Regarding the need to impose different obligations on initial and/or secondary controllers, Luxembourg opposes such hierarchisation of controllers. From the perspective of the data subject, such differentiation does not make sense and, worse, can be seen non-transparent if the right to erasure / be forgotten is not possible or rejected. Furthermore, it may well be that a data subject wishes to delete his data from a search engine but not from the original source, or vice versa. Luxembourg believes that the right to erasure / be forgotten should primarily be aimed at the controller, whose prime responsibility is also reflected in Article 26. This allows also for a more future-proof legislation, as the evolution of business models and agreements between various actors in the Internet value chain is impossible to foresee. On another note, Luxembourg welcomes the clarification from the EUCJ that a search engine is to be considered a controller

HUNGARY

Presidency proposal regarding the right to be forgotten

1. We share the Presidency's viewpoint about the need to adjust the planned legislation of the right to be forgotten and the right to erasure to the recent Google Spain judgement.
2. We support the reinsertion of the expression "relating to them" to Article 17 because it clarifies better the scope of the exercise of rights by the data subject. Nevertheless, we think that this expression does not relate to the personal data provider (data subject or third person), so in that aspect the reinsertion has no effect. At the same time we do agree with the interpretation that the scope of the right to be forgotten covers data disclosed by third person as well.
3. We do agree with the planned amendment of Article 17 para. 1. point a) and d) ("*by that controller*"), we believe that this addition gives a clear guidance in those cases when the primary and the secondary controller is not the same (i.e. the data is processed on different legal basis or for a different purpose).

The need to balance the right to the protection of personal data with the freedom of expression and the interest to access to information

4. We do agree with the concept being intrinsic to the regulation that the reconciliation of the right to the protection of personal data and the freedom of expression should remain in Member States' legislative power. This concept originates from the spirit of the founding treaties. However, Hungary notes that the national legislative power obviously will not lead to a unified application of law in this context.
5. We agree that the data subjects can exercise their right to be forgotten and right to erasure without an established order of requests to do it. This interpretation is in accordance with the Google Spain judgement.
6. We agree that Article 17 para. 2a. can be deleted, nevertheless, we would like to note that Hungary finds Article 17b essential, and hence it could not be omitted.

AUSTRIA

II. On 11289/14 (right to be forgotten)

Point 8 of the Presidency document

Austria sees no need to insert the words "relating to them", as they would not add any meaningful content.

Point 14 of the Presidency document

Austria does not consider that the judgment of the Court of Justice in Case C-131/12 has any direct effect on the system of provisions set out in Article 17 in conjunction with Article 19. However, we reserve the right in this context to make new proposals as to the wording of point (f) of Article 6(1).

Point 24 of the Presidency document

Austria is opposed to having different categories of controller.

The question of which of the obligations under Articles 17, 17a or 19 apply to a particular controller must be answered on the basis of the specific situation in each case – including in the context of the internet. As operators of search engines have the power to distribute information from other sources, specific obligations in respect of data subjects may apply to such operators. The Court of Justice has put forward conclusive arguments to that effect. Accordingly, there is no need for overall specific rules applicable to, for example, operators of search engines. However, it could be useful to have a recital offering an interpretation to explain how Article 17 and subsequent articles are to be applied correctly to search engines and social networks, using the Google judgment as an example.

Logically, the national legislator cannot be solely responsible for striking a balance between different fundamental rights – particularly given the Court of Justice's decisions in cases C-293/12 and C-594/12. The Union legislator, too, has a role to play in areas for which it is competent. Nevertheless, conflicts must generally be resolved on a case-by-case basis, starting with a problem that has arisen in the Member States and which may, in particular, be dealt with via the mechanism set out in Article 57.

Point 28 of the Presidency document

Austria assumes that Article 17(2a) relates to a situation in which a request for erasure made to an "initial publisher" (the controller who first made the data public; e.g. an online media undertaking) has been granted because the data subject's interests were considered to outweigh those of freedom of expression and of the press, making deletion of the source itself necessary.

In that case, it makes sense for the initial publisher to be obliged to inform the operator of a search engine, for example. That is the only way of ensuring that the latter can immediately update the search engine's cache to avoid a situation in which data deleted at the source can still be found via the search engine.

With those circumstances in mind, it would appear justified to let Article 17(2a) stand. A recital could provide clarification of the reasoning, along the lines set out above.

POLAND

In our opinion the judgment in case C-131/12 Google Spain **does not directly affect the concept of “right to be forgotten” embedded in Article 17.2a (originally art. 17.2) of the Regulation.** The right, the existence of which the ECJ inferred basing on Article 12 point b and Article 14 point a of Directive 95/46/EC, is in effect an extrapolation of the right to erasure and right to object to the processing of personal data. These two rights are already embodied in the draft Regulation in Article 17 paragraph 1 and Article 19 paragraph 1. Therefore, we see no direct relation between the “right to be forgotten” as it was established in the ECJ’s verdict, and the right to be forgotten introduced in Article 17 paragraph 2a of the draft Regulation and these two notions must not be confused. From our perspective the Google Spain judgment should be considered, *inter alia*, as extending the possibility to exercise of the **right to erasure** to search engines (and potentially other online service providers) which previously were not considered to be data controllers in relation to third party data. What is affected, therefore, is the notion of controller and we should focus on this issue in our future discussions.

With respect to **Article 17 paragraph 2a** of the draft Regulation, in our opinion it **should be deleted.** The current wording of this paragraph creates difficulties both for data subjects (by forcing unnecessary processing of otherwise dormant data, it threatens to create the so-called Barbra Streisand effect, moreover it creates an assumption that a data subject wants to execute his/her right to be forgotten against all the websites, not just selected ones) as well as data controllers (additional and ill-defined burdens, lack of certainty). At the same time, the information obligation established in this paragraph has a very broad scope – the number of data controllers that have to be informed might often be significant and include, for example, significant number of social networks’ users or webpage visitors. In the event that a majority of Member States will not support the deletion of Article 17 paragraph 2a, we propose an alternative wording to be considered. Our proposal aims to limit the number of data controllers which should be informed by the initial controller. Such restriction makes the right established by paragraph 2a feasible in practice. Under the proposed wording, the information duty is limited only to controllers to whom the data were intentionally disclosed by the initial controller and are therefore know to him/her:

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 controllers **to which he intentionally disclosed the data** ~~which are processing the data~~, that a data subject requests them to erase any links to, or copy or replication of that personal data.*

As regards the idea underlying paragraph 2a, in Poland's opinion we have to take into account that a data subject may want to delete his/her personal data only from a particular webpage or service, such as a search engine, not from everywhere. Only the data subjects know exactly what they want to do with their data. In practice there might be situations where a data subject wants to remove data only from selected controllers, for example webpage operators. To give an example: there is an old class photos on a school's website. A data subject, a former student of this school, now a respected businessman, may not want the picture to show up in a search results of Google Search or Bing, but he may have nothing against this picture remaining on the school's website or an online forum where former students communicate between each other. In Poland's opinion in such cases a data subject should have a choice to limit erasure to specified controllers.

The Presidency's document raises the issue of **de-ranking of search results** (referred in paragraph 22 of the document). In the Presidency's opinion "through the use of appropriate algorithms the search results concerning the data subject who had invoked the right to be forgotten (or to obscure the data) could be moved to subsequent pages in the search results, so as to hamper the finding of the person's data". Poland is against such a solution. In our opinion, Internet users can expect search results to be based on a neutral algorithm. Moreover, law which allows de-ranking of search results might constitute a dangerous precedent for the future, in particular in the context of **net neutrality**.

With respect to '**derogation' for journalistic purposes**, in the opinion of Poland this exception should be applied in each case which satisfies the conditions set for journalism. If the journalistic exception would cover only the initial data controllers (initial publishers of a given content) and not entities that for example facilitate access to information (or for example, base their activities on reprints, quotations, etc.), it could in some cases constitute a limitation to the journalistic activities, notably by limiting the public exposure of certain articles. At the same time we should bear in mind that providers of information society services can benefit from the limitations of liability, as provided in the eCommerce Directive 2000/31/EC. Finally, when dealing with any matters related to freedom of expression, we should remember that Article 80 of the draft Regulation explicitly mentions “journalistic purposes”. Therefore, all the Member States are obliged to adopt national laws which reconcile the right to protection of personal data with journalistic freedom. In practice, to facilitate this balance, Member States should adopt appropriate exemptions and derogations from specific provisions of the draft Regulation.

One of the most important issues raised in the Google Spain verdict is the **definition of a data controller**. The ECJ stated that Google acts as a controller of data processed by its search engine. The ECJ did not introduce a gradation of controllers or divide them into different groups. In the light of the above, we see no need for an introduction of a definition of a so-called “**secondary controller**” or establishing an order of controllers to be approached by a data subject. What the judgment in Google Spain case shows us, is that in the information society we will deal with various types of data controllers, including new types which will probably emerge in the future. This does not mean, however, that we should create a gradation of data controllers. As already mentioned above, data subjects should have free choice regarding erasure of their data, without the need to analyse whether they are dealing with an “initial” or a “secondary” controller, as only they know exactly what they want to do with their data (e.g. whether they want to limit erasure to specified controllers).

ROMANIA

Article 17 - Right to be forgotten and to erasure

Paragraph 1 - To better distinguish between the processing carried out by the first controller and second controller, we propose the following rewording:

1. **The initial controller or the second controller, depending on its involvement in the processing operations,** 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 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 **relating to them**;

Paragraph 1 (e)

Romania maintains its scrutiny reservation regarding this article. It is still not clear whether this paragraph applies to the public sector, in which case there could be difficulties in implementation, for example as regards the processing of personal data in criminal records.

SLOVAK REPUBLIC

Point 8 (First question)

We are not of the opinion that the term “relating to them” implies that personal data were provided by the data subject and this term does not limit the right to be forgotten to data provided solely by the data subject. Adding the term “relating to them” does not affect the right to be forgotten in a way which would imply that data were provided by the data subject versus provided by another subject. On the contrary, if the term “relating to them” should imply that the data subject has the right to request deletion of data provided solely by him/her it will limit this right in contrary with the aim of the proposal for the Regulation and opinion of the Court of Justice in ruling against Google Spain. We therefore deem it not necessary to add this provision since it is not relevant in the context of the right to be forgotten and the explanation of the recital with regard to personal data being the data related to the data subject is satisfactory.

Point 14 (Second question)

Article 17 (1) (a) and (b) in our opinion corresponds with the ruling of the Court of Justice and its further modification is not necessary.

Point 24 (Third question)

We can express positive attitude towards both sub-questions of the PRES and therefore we agree that the role of reconciliation of the right to the protection of personal data and the right to freedom of expression should be on Member State’s responsibility. Similarly we can agree with statement that the data subject should have the possibility to execute his/her right to be forgotten with no regards to order of the controllers towards which this right might be applicable.

Point 28 (Fourth question)

We fully agree with opinion of IE delegation that the provision of Article 17 (2a) does not correspond with recital 54. Recital 54 addresses obligation of other controllers to delete data based on the notification of original controller while Article 17 (2a) addresses original controller’s obligation to notify these other controllers. This discrepancy must be solved and it is necessary to determine the aim of Article 17 (2a). In case the other controllers are not obliged to delete these data than this provision is redundant and its contribution to data subject’s rights is questionable.