FUNDACJA PANOPTYKON

Comments on the „right to be forgotten"

Note: this is a working document, drafted for discussion with Google advisory board.

Terminology and separation of different legal regimes

There is a lot of confusion around the so-called „right to be forgotten". It seems more practicable and correct in terms of existing legal framework to refer to the **existing and unquestionable right to data correction and erasure**. All data subjects have these rights and all data controllers are obliged to respect them. In this sense, there is no need to fundamentally change the existing data protection framework. The whole **debate on „right to be forgotten" should rather be seen as concerning implementation and interpretation of these existing rights with regard to internet intermediaries**. It should also be kept separate from the discussion on art. 17 of the draft data protection regulation (pending proposal on the EU level), which offers yet another understanding of the „right to be forgotten". We must also remember that the alternative to placing an obligation on search engines to correct unfair, out of date results is to allow them to cause this prejudice to individuals.

It is important to realise that there are three distinct (yet overlapping) legal regimes:

(i) rights and obligations arising under data protection regime (on EU level Data Protection Directive);

(ii) rights and obligations arising under the law on the provision of electronic services (on EU level e-Commerce Directive), in particular so called notice and take-down procedure;

(iii) legal claims arising on the grounds of general civil law, in particular the protection of privacy and other rights (in Polish law referred as "personal goods").

The Court of Justice of the EU in its judgement only referred to data protection regime. But in the debate many actors seem to refer to other regimes, which leads to confusion. Therefore, it seems important to stress that rights and obligations that exist under data protection regime are fundamental rights, are not negotiable and should not be questioned in this debate.

In legal terms, we should only be discussing the enforcement of data protection regime. However, because some practical questions cannot be answered by a simple reference to data protection law, what can also be discussed is **how the experience of internet intermediaries arising from legally binding notice and take-down procedures (as opposed to voluntary measures applied by the intermediaries) or dealing with civil claims could be used to ensure better implementation of the data protection regime**. What counterbalancing measures can be envisaged to ensure that intermediaries do not over-implement such orders like the one given in Costeja case?

Search engines as data controllers

We understand that the purpose of the public debate started by Google is **not** to question the decision of the ECJ that search engines should be treated as data controllers. Nevertheless, it seems

important to clarify the implications of such decision. All the more that some actors in the debate seem to suggest that as a result of this decision search engines became legally liable for all personal data processed and published online, which is not the case.

Search engines are free to determine the process of indexing online content, the algorithms used for selecting it in response to search queries, and the way it is presented on their websites. Therefore, they should be treated as data controllers as long as any of these activities involve data processing.

It does not mean, however, that search engines become liable for the way that personal data is processed by any other entity or website. It is clear on the grounds of Costeja case, where Google was only ordered to modify the way its search results are presented as a result of searches based on Mr Costeja's name, but not the way in which personal data is processed on the original website.

Deletion of content versus modification of search results

Even though Google advisory board does not consider this as an issue, it seems important to reinforce in the debate triggered by ECJ's decision that **search engines are not expected to "delete content"** (it would be technically impossible) **nor remove pages from its index (rendering them "unfindable" through Google – despite the "notices of removal from Google search" that have been sent by Google to webmasters.**

They are only required to **modify search results so that personal data are no longer processed if (and only if) such processing would infringe the existing law and only in relation to searches based on the individual's name**. In practice it means that certain search results will not be presented in response to queries based on the name of the individual that has made the complaint. It may seem obvious for the panel of experts, but certainly is not obvious for Internet users and citizens following the debate.

How to avoid arbitrary decisions? What procedural safeguards can be introduced?

In the first place it should be noted that nothing in the ECJ judgement suggests that search engines should react automatically to data subjects' requests regarding correction or deletion of their personal data from search results. On the contrary: **data controller should always verify whether conditions for exercising data subject's right to correct or erase personal data are met**. In the context of on-line publications, the scope of the so called journalistic exemption will always come into play. Data controller could also argue that the right to erasure cannot be exercised because there are legitimate grounds for further data processing (such as legitimate interests of third parties and other individuals).

In practice, it means that **data controller has to verify on a case-by-case basis whether the right to free expression or other rights of other individuals may prevent the data subject from exercising his/her right to erase personal data**. The Court ruling creates an incentive for Google to restrict access to content, but identifies no counterbalancing obligation to prevent over-implementation.

This correction/erasure obligation exists in current data protection regime and therefore is nothing new. What adds more complexity in the case of Google and other search engines, however, is the

fact that (as a matter of rule) search engines process personal data that were made public by a different entity (so called primary data controller).

Taking into account the nature of the relationship between primary data controller (publisher), secondary data controller (search engine) and the data subject, essentially, there are two possible scenarios:

1. The primary data controller **receives a request to erase data from the data subject and complies with it**. In this case the search engine should always follow and adjust search results accordingly. They have an obvious business interest in doing this, in order to ensure that their search results are up to date.
2. The primary controller **does not receive data erasure request** (for example because data subject is not interested in removing data from the source website but only wants to remove it from search results) **or refuses to comply with it** (for example on the grounds of journalistic exemption or other legitimate interest of third parties/individuals – exactly like in Costeja case). In this case, the **secondary data controller should carry out its independent assessment and apply the data protection law accordingly**. Such independent assessment is needed because the purposes of data processing by the secondary controller are different. Therefore, it might be the case that the same exemption as relied on by the primary controller will not apply to the processing by the secondary controller. In the Costeja case, the original article did not breach the law. However, the search results being generated by searches on his name were out of date and prejudicial.

Because only the second scenario seems to be problematic, we will focus our further analysis on this type of cases.

i. Referring the case to Data Protection Authority

Data controllers can refer their disputes with data subjects to a Data Protection Authority and seek advice, interpretation or even wait with their own actions for its binding decision. In any case of interpretative doubts, this route should be followed.

Moreover, Art 29 Working Party has just released detailed guidelines that will be helpful in determining when a journalistic exemption or other legitimate interest of third parties/individuals can be applied to reject a data erasure request.

ii. Using experience from notice and take-down procedure

Google and other search engines could use their experience from dealing with requests received under legally-binding notice and take-down procedure. It must be noted that existing US law (DCMA) requires search engines to completely de-index links to content that infringes copyright law. In fact, these obligations go considerably further that what is required in accordance with recent ECJ judgement.

Without prejudice to the rights of data subjects arising under the data protection regime**, procedures developed under legally binding notice and take-down regime**[1] **could be used in**

[1] Please note that we do *not* refer here to voluntary measures and practices developed by internet intermediaries outside of any legal framework, which may often amount to arbitrary decisions. To the best of our knowledge, Google not only deals with requests sent in accordance with US law (implementing them on a global level) but

order to verify whether the free expression exemption applies in a given case. In other words, by inviting comments/interventions from the primary data controllers (publishers), search engines can avoid taking arbitrary decisions with regard to the application of journalistic exemption or other legitimate interest of third parties/individuals. **Ultimately, however, it is the search engine's responsibility (as the data controller) to interpret and apply data protection law. Such decisions can not be avoided by referring every single case to the Data Protection Authority because it would effectively limit data subject's right to data erasure.**

iii. Detailed recommendations:

- As a matter of a good practice, the secondary controller (search engine) should consult the primary data controller (publisher) in order to determine whether there is a public interest in further processing of personal data (under journalistic exemption or other legitimate interest of third parties/individuals) .
- Existing jurisprudence, in particular the guidelines set by the European Court for Human Rights, should be followed by the data controller when determining the scope of journalistic or other exemptions from the right to data erasure.
- If the secondary controller (search engine) on the basis of its own assessment decides not to modify search results , it should give the data subject detailed guidelines on how to refer the case to relevant Data Protection Authority ("right to appeal").
- If the secondary controller (search engine) on the basis of its own assessment decides to modify search results, the primary controller (publisher) should be notified.
- Factors that are not considered relevant in the data protection law, such as format of personal data (picture or text) , should not be taken into account in determining the scope of journalistic exemption or other legitimate interest of third parties/individuals in a given case.
- The fact whether a data subject in question is private or public person is certainly relevant for determining the scope of journalistic exemption but should not be seen as the only relevant factor (i.e. also public persons have the right to erase their personal data if processing of such data does not serve public interest).
- Legitimate interests of the society such as national security concerns or access to scientific knowledge should be taken into account in determining the scope of journalistic exemption or other legitimate interest of third parties/individuals in a given case in a given case.

---

also takes voluntary actions with regard to other types of disputed content globally and on a national level (the letter sent to Google advisory board by European Digital Rights develops more on this particular issue).