ARTICLE 29 DATA PROTECTION WORKING PARTY

14/EN
WP 225

GUIDELINES ON THE IMPLEMENTATION OF THE COURT OF JUSTICE OF THE EUROPEAN UNION JUDGMENT ON "GOOGLE SPAIN AND INC V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ" C-131/12

Adopted on 26 November 2014

EXECUTIVE SUMMARY

1. Search engines as data controllers

The ruling recognises that search engine operators process personal data and qualify as data controllers within the meaning of Article 2 of Directive 95/46/EC. The processing of personal data carried out in the context of the activity of the search engine must be distinguished from, and is additional to that carried out by publishers of third-party websites.

2. A fair balance between fundamental rights and interests

In the terms of the Court, "in the light of the potential seriousness of the impact of this processing on the fundamental rights to privacy and data protection, the rights of the data subject prevail, as a general rule, over the economic interest of the search engine and that of internet users to have access to the personal information through the search engine". However, a balance of the relevant rights and interests has to be made and the outcome may depend on the nature and sensitivity of the processed data and on the interest of the public in having access to that particular information. The interest of the public will be significantly greater if the data subject plays a role in public life.

3. Limited impact of de-listing on the access to information

In practice, the impact of the de-listing on individuals' rights to freedom of expression and access to information will prove to be very limited. When assessing the relevant circumstances, DPAs will systematically take into account the interest of the public in having access to the information. If the interest of the public overrides the rights of the data subject, de-listing will not be appropriate.

4. No information is deleted from the original source

The judgment states that the right only affects the results obtained from searches made on the basis of a person's name and does not require deletion of the link from the indexes of the search engine altogether. That is, the original information will still be accessible using other search terms, or by direct access to the publisher's original source.

5. No obligation on data subjects to contact the original website

Individuals are not obliged to contact the original website in order to exercise their rights towards the search engines. Data protection law applies to the activity of a search engine acting as a controller. Therefore, data subjects shall be able to exercise their rights in accordance with the provisions of Directive 95/46/EC and, more specifically, of the national laws that implement it.

6. Data subjects' entitlement to request delisting

Under EU law, everyone has a right to data protection. In practice, DPAs will focus on claims where there is a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident of an EU Member State.

7. Territorial effect of a de-listing decision

In order to give full effect to the data subject's rights as defined in the Court's ruling**,** de-listing decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.

8. Information to the public on the delisting of specific links

The practice of informing the users of search engines that the list of results to their queries is not complete as a consequence of the application of European data protection law based on any no legal requirement under data protection rules. Such a practice would only be acceptable if the information is presented in such a way that users cannot, in any case, conclude that one particular individual has asked for the removal of results concerning him or her.

9. Communication to website editors on the delisting of specific links

Search engines should not as a general practice inform the webmasters of the pages affected by removals of the fact that some web pages cannot be acceded from the search engine in response to a specific name-based query. There is no legal basis for such routine communication under EU data protection law.

In some cases, search engines may want to contact the original editor in relation to particular request prior to any delisting decision, in order to obtain additional information for the assessment of the circumstances surrounding that request.

Taking into account the important role that search engines play in the dissemination and accessibility of information posted on the Internet and the legitimate expectations that webmasters may have with regard to the indexing and presentation of information in response to users' queries, the Working Party 29 (hereinafter: the Working Party) strongly encourages the search engines to provide the delisting criteria they use, and to make more detailed statistics available.

TABLE OF CONTENTS

PART I: Interpretation of the CJEU Judgment

This document is designed to provide information as to how the European Data Protection Authorities ("DPAs") assembled in the Article 29 Working Party intend to implement the judgment of the Court of Justice of the European Union (hereinafter: CJEU) in the case of "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" (C-131/12). It also contains the list of common criteria which the DPAs will apply to handle the complaints, on a case-by-case basis, filed with their national offices following refusals of de-listing by search engines. The list of criteria should be seen as a flexible working tool which aims at helping DPAs during the decision-making processes. The criteria will be applied in accordance with the relevant national legislations. No single criterion is, in itself, determinative. The list of criteria is non-exhaustive and will evolve over time, building on the experience of DPAs.

A. Search engines as controllers and legal ground

1. The ruling recognizes that search engine operators process personal data and do it as controllers in the meaning of articles 2 of Directive 95/46 (Paragraphs 27, 28 and 33).

2. The processing of personal data carried out in the context of the activity of the search engine can be distinguished from and is additional to that carried out by publishers of websites, which consists in loading the data on an internet page (Paragraph 35).

3. The legal ground for that processing under the EU Directive is to be found in Article 7(f), the necessity for the legitimate interest of the controller or of the third parties to which data are disclosed (Paragraph 73).

4. The processing carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (Paragraph 80).

5. In relation to the balance of interests that may legitimate the processing carried out by the search engine, according to the ruling, the rights of the data subject prevail as a general rule, over the economic interest of the search engine, in light of the of the potential seriousness of the impact of this processing on the fundamental rights to privacy and data protection. These rights also generally prevail over the rights of internet users to have access to the personal information through the search engine in a search on the basis of the data subject's name. However, a balance has to be struck between the different rights and interests and the

outcome may depend on the nature and sensitivity of the processed data and on the interest of the public to have access to that particular information on the other, an interest which may vary, in particular, by the role played by the data subject in public life (Paragraph 81).

6. Data subjects have the right to request and, if the conditions laid down by articles 12 and 14 of Directive 95/46 are met, to obtain the removal of links to web pages published by third parties containing information relating to them from the list of results displayed following a search made on the basis of a person's name.

7. The respective legal grounds of original publishers and search engines are different. The search engine should carry out the assessment of the different elements (public interest, public relevance, nature of the data, actual relevance…) on the basis of its own legal ground, which derives from its own economic interest and that of the users to have access to the information via the search engines and using a name as terms of search. Even when (continued) publication by the original publishers is lawful, the universal diffusion and accessibility of that information by a search engine, together with other data related to the same individual, can be unlawful due to the disproportionate impact on privacy.

The ruling does not oblige search engines to permanently carry out that assessment in relation to all the information they process, but only when they have to respond to data subjects' requests for the exercise of their rights.

8. The interest of search engines in processing personal data is economic. But there is also an interest of internet users in receiving the information using the search engines. In that sense, the fundamental right of freedom of expression, understood as "the freedom to receive and impart information and ideas" in article 11 of the European Charter of Fundamental Rights, has to be taken into consideration when assessing data subjects' requests.

9. The impact of the exercise of individuals' rights on the freedom of expression of original publishers and users will generally be very limited. Search engines must take the interest of the public into account in having access to the information in their assessment of the circumstances surrounding each request. Results should not be delisted if the interest of the public in having access to that information prevails. But even when a particular search result is delisted, the content on the source website is still available and the information may still be accessible through a search engine using other search terms.

B. Exercise of rights

10. Data Protection law applies to the activity of a search engine acting as a controller. Therefore, data subjects should be able to exercise their rights in accordance with the provisions of Directive 95/46 and, more specifically, of the national laws that implement it.

11. Individuals are not obliged to contact the original site, either previously or simultaneously, in order to exercise their rights towards the search engines. There are two different processing operations, with differentiated legitimacy grounds and also with different impacts on the individual's rights and interests. The individual may consider that it is better, given the circumstances of the case, to first contact the original webmaster to request the deletion of

information or the application of "no index" protocols to it, but the judgment does not require this.

12. By the same reason, an individual may choose how to exercise his or her rights in relation to search engines by selecting one or several of them. By making a request to one or several search engines the individual is making an assessment of the impact of the appearance of the controverted information in one or several of the search engines and, consequently, makes a decision on the remedies that may be sufficient to diminish or eliminate that impact.

13. While Directive 95/46 does not contain specific provisions on the means for the exercise of rights, most national data protection laws provide for great flexibility in that regard and offer data subjects the possibility of lodging their requests in a variety of ways, irrespective of the fact that the controller may have established "ad hoc" procedures.

Consequently, and as a best practice that would be in line with all possible legal requirements in all EU Member States, data subjects should be able to exercise their rights with search engine operators using any adequate means. Although the use of specific mechanisms that may be developed by search engines, namely online procedures and electronic forms, may have advantages and would be advisable because of its convenience, it should not be the exclusive way for data subjects to exercise their rights.

14. For the same reasons, search engines must follow national data protection laws with regard to the requirements for making a request and for the timeframes and contents of the answers. In particular, when a data subject requests delisting of some links, some form of identification may be demanded by the data controller, but, again, in line with what national laws consider necessary and proportionate in order to verify the identity of the applicant in the context of the request. When the controller collects identification information, adequate safeguards should be in place.

In order for the search engine to be able to make the required assessment of all the circumstances of the case, data subjects must sufficiently explain the reasons why they request delisting, identify the specific URLs and indicate whether they fulfill a role in public life, or not.

15 When a search engine refuses a delisting request, it should provide sufficient explanation to the data subject about the reasons for the refusal. It should also inform data subjects that they can turn to the data protection authority or to court if they are not satisfied with the answer. Such explanations should also be provided by data subjects to the DPA, in case they decide to refer to it.

16. The ruling considers that Google's national subsidiaries in the EU are establishments of the company and that Google's personal data processing in the search engine is carried out in the context of activities of these establishments which makes EU data protection rules applicable.

Directive 95/46 does not contain any specific provision with regard to the responsibility of establishments of the controller located in the territory of Member States. The only reference

is in article 4.1.a, that states that "when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable". This provision is to some extent clarified by Recital 19: "when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;"

The effective application of the ruling and of data protection law requires that data subjects may exercise their rights with the national subsidiaries of search engines in their respective Member States of residence, and also that DPAs may contact their respective national subsidiaries in relation to requests or complaints lodged by data subjects.

These subsidiaries are of course free to follow internal procedures to deal with the requests, either directly or by forwarding the requests to other establishments of the company. It might also be reasonable to expect that as a first reaction they advise data subjects to use the "ad hoc" procedures developed by the company and the corresponding electronic forms. But if the data subject insists in contacting the national subsidiary they should not reject the request.

C. Scope

17. The ruling is specifically addressed to generalist search engines, but that does not mean that it cannot be applied to other intermediaries. The rights may be exercised whenever the conditions established in the ruling are met.

18. Search engines included in web pages do not produce the same effects as "external" search engines. On the one hand, they only recover the information contained on specific web pages. On the other, and even if a user looks for the same person in a number of web pages, internal search engines will not establish a complete profile of the affected individual and the results will not have a serious impact on him, Therefore, as a rule the right to de-listing should not apply to search engines with a restricted field of action, particularly in the case of search tools of websites of newspapers.

19. Article 8 of the EU Charter, to which the ruling explicitly refers in a number of paragraphs, to, recognizes the right to data protection to "everyone". In practice, DPAs will focus on claims where there is a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident of an EU Member State.

20. As stated by the Court, EU law applies, and the ruling must be implemented with regard to the processing operation that consists in "finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference"

The CJEU maintains that "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, published by third parties and containing information relating to that person".

Finally, the Court also states that "the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved."

The ruling sets thus an obligation of results which affects the whole processing operation carried out by the search engine. The adequate implementation of the ruling must be made in such a way that data subjects are effectively protected against the impact of the universal dissemination and accessibility of personal information offered by search engines when searches are made on the basis of the name of individuals.

Although concrete solutions may vary depending on the internal organization and structure of search engines, de-listing decisions must be implemented in a way that guarantees the effective and complete protection of these rights and that EU law cannot be easily circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the judgment. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.

21. From the material point of view, and as it's been already mentioned, the ruling expressly states that the right only affects the results obtained on searches made by the name of the individual and never suggests that the complete deletion of the page from the indexes of the search engine is needed. The page should still be accessible using any other terms of search. It is worth mentioning that the ruling uses the term "name", without further specification. It may be thus concluded that the right applies to possible different versions of the name, including also family names or different spellings

D. Communication to third parties

22. It appears that some search engines have developed the practice of systematically informing the users of search engines of the fact that some results to their queries have been delisted in response to requests of an individual. If such information would only be visible in search results where hyperlinks were actually delisted, this would strongly undermine the purpose of the ruling. Such a practice can only be acceptable if the information is offered in such a way that users cannot in any case come to the conclusion that a specific individual has asked for the delisting of results concerning him or her.

The use of notices or statements should be made in a consistent way in order to prevent users from coming to wrong or incorrect assumptions. Given the difficulties that managing these statements on the basis of a specific type of search terms (i.e. whenever names are used)

entails, it is advisable that this information is provided via a general statement permanently inserted on search engines' web pages.

23. Search engine managers should not as a general practice inform the webmasters of the pages affected by removals of the fact that some webpages cannot be acceded from the search engine in response to specific queries. Such a communication has no legal basis under EU data protection law.

As stated before, there is a crucial difference between the legal ground for the processing by search engines, and the legal ground for the processing by the original publisher. Article 7.f serves as the legal ground for processing operations which are necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. The interest of the original webmasters in receiving the communication is questionable for a number of reasons. On the one hand, the delisting of a hyperlink in a search result in a search for a person's name only has limited impact, as described before. On the other hand, original webmasters cannot make an effective use of the communication received, as it affects a processing operation carried out by the controller over which they have no control or influence. As a matter of fact, search engines do not recognize a legal right of publishers to have their contents indexed and displayed, or displayed in a particular order.

In any case, that interest should be balanced with the rights, freedoms and interests of the affected data subject.

No provision in EU data protection law obliges search engines to communicate to original webmasters that results relating to their content have been delisted. Such a communication is in many cases a processing of personal data and, as such, requires a proper legal ground in order to be legitimate. No legal ground can be found in article 7 of Directive 95/46 to routinely communicate de-listing decisions to primary controllers.

On the other hand, it may be legitimate for search engines to contact original publishers prior to any decision about a delisting request, in particularly difficult cases, when it is necessary to get a fuller understanding about the circumstances of the case. In those cases, search engines should take all necessary measures to properly safeguard the rights of the affected data subject.

Taking into account the important role that search engines play in the dissemination and accessibility of information posted on the Internet and the legitimate expectations that webmasters may have with regard to the indexation of information and display in response to users' queries, the Working Party strongly encourages the search engines to publish their own delisting criteria, and make more detailed statistics available.

E. Role of the DPAs

24. Despite the novel elements of the CJEU judgment, deciding whether a particular search result should be delisted involves – in essence - a routine assessment of whether the processing of personal data done by the search engine complies with the data protection principles. Therefore the Article 29 Working Group considers that complaints submitted by data subjects to DPAs in respect of refusals or partial refusals by search engines are to be treated – as far as is possible - as formal claims as envisaged by Article 28(4) of the Directive. Accordingly, such appeals should normally be treated by DPAs under their national legislation in the same manner as all other claims/complaints/requests for mediation.

25. The Chair of the Working Party will contact search engines in order to clarify which EU establishment should be contacted by the competent DPA and will make the results of the consultation public if necessary.

PART II: List of common criteria for the handling of complaints by European data protection authorities

In its decision on 13 May 2014, the CJEU clarified the application of data protection law of to search engines. It concluded that users can request search engines, under certain conditions, to delist certain links to information affecting their privacy from the results for searches made against their name. Where a search engine refuses such a request, the data subject may bring the matter before the DPAs, or the relevant judicial authority, so that they carry out the necessary checks and take a decision in accordance with their power in national law

It follows from the CJEU judgment that a data subject may "request [from a search engine] that the information [relating to him personally] no longer be made available to the general public on account of its inclusion in […] a list of results". The Court also ruled that "those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name". This right is recognised by the CJEU in the light of the fundamental rights granted under Articles 7 and 8 of the European Charter of Fundamental Rights and in application of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC ("the Directive").

The Court also recognised the existence of an exception to this general rule when "for particular reasons, such as the role played by the data subject in public life […], the interference with [the] fundamental rights [of the data subject] is justified by the preponderant interest of the general public in having, on account of [the] inclusion [of the information] in the list of results, access to the information in question".

A first analysis of the complaints so far received from data subjects whose delisting requests were refused by the search engines, has enabled DPAs to establish a list of common criteria to be used by them to evaluate whether data protection law has been complied with. DPAs will assess complaints on a case-by-case basis, using the criteria below.

The list of criteria should be seen as a flexible working tool which will help DPAs during their decision-making process. The criteria will be applied in accordance with the relevant national legislation.

In most cases, it appears that more than one criterion will need to be taken into account in order to reach a decision. In other words, no single criterion is, in itself, determinative.

Each criterion has to be applied in the light of the principles established by the CJEU and in particular in the light of the "the interest of the general public in having access to [the] information".

CRITERIA	COMMENT
1. Does the search result relate to a natural person – i.e. an individual? And does the search result come up against a search on the data subject's name?	The Google judgment recognised the particular impact that an internet search, based on an individual's name, can have on his or her right to respect for private life. DPA's will also consider pseudonyms and nicknames as relevant search terms when the individual can establish that they are linked to his/her real identity.
2. Does the data subject play a role in public life? Is the data subject a public figure?	The CJEU has made an exception for delisting requests from data subjects that play a role in public life, where there is an interest of the public in having access to information about them. This criterion is broader than the 'public figures' criterion. **What constitutes "a role in public life"?** It is not possible to establish with certainty the type of role in public life an individual must have to justify public access to information about them via a search result. However, by way of illustration, politicians, senior public officials, business-people and members of the (regulated) professions can usually be considered to fulfill a role in public life. There is an argument in favour of the public being able to search for information relevant to their public roles and activities. A good rule of thumb is to try to decide where the public having access to the particular information – made available through a search on the data subject's name – would protect them against improper public or professional conduct. It is equally difficult to define the subgroup of 'public figures'. In general, it can be said that public figures are individuals who, due to their functions/commitments, have a degree of media exposure.

	The Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy provides a possible definition of "public figures". It states that "Public figures are persons holding public office and/or using public resources and, more broadly speaking, all those who play a role in public life, whether in politics, the economy, the arts, the social sphere, sport or in any other domain." There may be information about public figures that is genuinely private and that should not normally appear in search results, for example information about their health or family members. But as a rule of thumb, if applicants are public figures, and the information in question does not constitute genuinely private information, there will be a stronger argument against de-listing search results relating to them. In determining the balance, the Jurisprudence of the European Court on Human Rights (hereinafter: ECHR) is especially relevant. **ECHR, van Hannover v. Germany, 2012**: "The role or function of the person concerned and the nature of the activities that are the subject of the report and/or photo constitute another important criterion, related to the preceding one. In that connection a distinction has to be made between private individuals and persons acting in a public context, as political figures or public figures. Accordingly, whilst a private individual unknown to the public may claim particular protection of his or her right to private life, the same is not true of public figures (see Minelli v. Switzerland (dec.), no. 14991/02, 14 June 2005, and Petrenco, cited above, § 55). A fundamental distinction needs to be made between reporting facts capable of contributing to a debate in a democratic society, relating to politicians in the exercise of their official functions for example, and reporting details of the private life of an individual who does not exercise such functions (see Von Hannover, cited above, § 63, and Standard Verlags GmbH, cited above, § 47)."[1]

[1] See also ECHR, Axel Springer v. Germany, 2012

3. Is the data subject a minor?	As a general rule, if a data subject is legally under age – e.g. is he or she is not yet 18 years old at the time of the publication of the information – DPAs are more likely to require de-listing of the relevant results. The concept of "best interests of the child" has to be taken into account by DPAs. This concept can be found, *inter alia*, in article 24 of Charter of fundamental rights of the EU: "In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration".
4. Is the data accurate?	In general, 'accurate' means accurate as to a matter of fact. There is a difference between a search result that clearly relates to one person's opinion of another person and one that appears to contain factual information. In data protection law the concepts of accuracy, adequacy and incompleteness are closely related. DPAs will be more likely to consider that de-listing of a search result is appropriate where there is inaccuracy as to a matter of fact and where this presents an inaccurate, inadequate or misleading impression of an individual. When a data subject objects to a search result on the grounds that it is inaccurate, the DPAs can deal with such a request if the complainant provides all the information needed to establish the data are evidently inaccurate. In cases where a dispute about the accuracy of information is still ongoing, for example in court or when there is on on-going police investigation, DPAs may choose not to intervene until the process is complete.
5. Is the data relevant and not excessive? **a. Does the data relate to the working life of the data subject?**	The overall purpose of these criteria is to assess whether the information contained in a search result is relevant or not according to the interest of the general public in having access to the information. Relevance is also closely related to the data's age. Depending on the facts of the case,

b. Does the search result link to information which is allegedly constitutes hate speech/slander/libel or similar offences in the area of expression against the complainant? **c. Is it clear that the data reflect an individual's personal opinion or does it appear to be verified fact?**	information that was published a long time ago, e.g. 15 years ago, might be less relevant that information that was published 1 year ago. The DPA's will assess relevance in accordance with the factors set out below. **a. Does the data relate to the working life of the data subject?** An initial distinction between private and professional life has to be made by DPAs when they examine de-listing request. Data protection - and privacy law more widely - are primarily concerned with ensuring respect for the individual's fundamental right to privacy (and to data protection). Although all data relating to a person is personal data, not all data about a person is private. There is a basic distinction between a person's private life and their public or professional persona. The availability of information in a search result becomes more acceptable the less it reveals about a person's private life. As a general rule, information relating to the private life of a data subject who does not play a role in public life should be considered irrelevant. However, public figures also have a right to privacy, albeit in a limited or modified form. Information is more likely to be relevant if it relates to the current working life of the data subject but much will depend on the nature of the data subject's work and the legitimate interest of the public in having access to this information through a search on his or her name. Two additional questions are relevant here: - Is data about a person's work related activity excessive? - Is the data subject still engaged in the same professional activity?

	b. Does the search result link to information which is excessive or allegedly constitutes hate speech/slander/libel or similar offences in the area of expression against the complainant? DPAs are generally not empowered and not qualified to deal with information that is likely to constitute a civil or criminal 'speech' offence against the complainant, such as hate speech, slander or libel. In such cases, DPAs will likely refer the data subject to the police and/or to court if a delisting request is refused. The situation would be different if a court had ordered that the publication of the information is indeed a criminal offence, or in violation of other laws. Nevertheless, DPAs remain competent to assess whether data protection law has been complied with. **c. Is it clear that the data reflect an individual's personal opinion or does it appear to be verified fact?** The status of the information contained in a search result mays also be relevant, in particular the difference between personal opinion and verified fact. DPAs recognise that some search results will contain links to content that may be part of a personal campaign against someone, consisting of 'rants' and perhaps unpleasant personal comments. Although the availability of such information may be hurtful and unpleasant, this does not necessarily mean that DPAs will consider it necessary to have the relevant search result delisted. However, DPAs will be more likely to consider the de-listing of search results containing data that appears to be verified fact but that is factually inaccurate.
6. Is the information sensitive in the meaning of Article 8 of the Directive?	As a general rule, sensitive data (defined in Article 8 of the Data Protection Directive as 'special categories of data') has a greater impact on the data subject's private life than 'ordinary' personal data. A good example would be information about a person's health, sexuality or religious beliefs. DPAs are more likely to intervene when delisting requests are refused in respect of

	search results that reveal such information to the public.
7. Is the data up to date? Is the data being made available for longer than is necessary for the purpose of the processing?	As a general rule, DPAs will approach this factor with the objective of ensuring that information that is not reasonably current and that has become inaccurate because it is out-of-date is de-listed. Such an assessment will be dependent on the purpose of the original processing.
8. Is the data processing causing prejudice to the data subject? Does the data have a disproportionately negative privacy impact on the data subject?	There is no obligation for the data subject to demonstrate prejudice in order to request de-listing, in other words prejudice is not a condition for exercising the right recognised by the CJEU. However, where there is evidence that the availability of a search result is causing prejudice to the data subject, this would be a strong factor in favour of de-listing.[2] The Directive allows the data subject to object to processing where there are compelling legitimate grounds for doing so. Where there is a justified objection, the data controller must cease processing the personal data. The data might have a disproportionately negative impact on the data subject where a search result relates to a trivial or foolish misdemeanor which is no longer – or may never have been – the subject of public debate and where there is no wider public interest in the availability of the information.
9. Does the search result link to information that puts the data subject at risk?	DPAs will recognise that the availability of certain information through internet searches can leave data subjects open to risks such as identity theft or stalking, for example. In such cases, where the risk is substantive, DPAs are likely to consider that the de-listing of a search result is appropriate.

[2]CJUE, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 13 May 2014, para. 96, **"it must be pointed out that it is not necessary in order to find such a right that the inclusion of the information in question in the list of results causes prejudice to the data subject."**

10. In what context was the information published? **a. Was the content voluntarily made public by the data subject?** **b. Was the content intended to be made public? Could the data subject have reasonably known that the content would be made public?**	If the only legal basis for personal data being available on the internet is consent, but the individual then revokes his or her consent, then the processing activity – i.e. the publishing – will lack a legal basis and must therefore cease. When assessing requests, the DPA will consider whether the link should be delisted even when the name or information is not erased beforehand or simultaneously from the original source In particular, if the data subject consented to the original publication, but later on, is unable to revoke his or her consent, and a delisting request is refused, the DPAs will generally consider that de-listing of the search result is appropriate.
11. Was the original content published in the context of journalistic purposes?	DPAs recognise that depending on the context, it may be relevant to consider whether the information was published for a journalistic purpose. The fact that information is published by a journalist whose job is to inform the public is a factor to weigh in the balance. However, this criterion alone does not provide a sufficient basis for refusing a request, since the ruling clearly distinguishes between the legal basis for publication by the media, and the legal basis for search engines to organise search results based on a person's name.
12. Does the publisher of the data have a legal power – or a legal obligation – to make the personal data publicly available?	Some public authorities are under a legal duty to make certain information about individuals publicly available – for example for electoral registration purposes. This varies according to Member State law and custom. Where this is the case, DPAs may not consider that de-listing is appropriate whilst the requirement on the public authority to make the information publicly available persists. However, this will have to be assessed on a case-by-case basis, together with the criteria of 'outdatedness' and irrelevance.

	DPAs may consider that de-listing is appropriate even if there is a legal obligation to make the content available on the original website.
13. Does the data relate to a criminal offence?	EU Member States may have different approaches as to the public availability of information about offenders and their offences. Specific legal provisions may exist which have an impact on the availability of such information over time. DPAs will handle such cases in accordance with the relevant national principles and approaches. As a rule, DPAs are more likely to consider the de-listing of search results relating to relatively minor offences that happened a long time ago, whilst being less likely to consider the de-listing of results relating to more serious ones that happened more recently. However, these issues call for careful consideration and will be handled on a case-by-case basis.