GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

italian version

[doc. web n. 3295641]

Decision Setting forth Measures Google Inc. Is Required to Take to Bring the Processing of Personal Data under Google's New Privacy Policy into Line with the Italian Data Protection Code -10 July 2014

THE GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Having convened today, in the presence of Mr. Antonello Soro, President, Ms. Augusta Iannini, Vice-President, Ms. Giovanna Bianchi-Clerici and Prof. Licia Califano, Members, and Mr. Giuseppe Busia, Secretary General;

Having regard to Directive 95/46/EC of 24 October 1995, 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;

Having regard to Directive 2002/58/EC of 12 July 2002, of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the electronic communications sector;

Having regard to Directive 2009/136/EC of 25 November 2009, of the European Parliament and of the Council, amending directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws;

Having regard to the Personal Data Protection Code (legislative decree No 196 of 30 June 2003, hereinafter the *Code*);

Having regard to legislative decree no 69 of 28 May 2012 "Amendments to legislative decree No 196 of 30 June 2003, containing the Personal Data Protection Code, in pursuance of Directive 2009/136/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector, and Directive 2009/140/EC on a common regulatory framework for electronic communications services, and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws" as published in Italy's Official Journal No 126 of 31 May 2012;

Having regard to the judgment issued by the Court of Justice of the EU on 13 May 2014, case C-131/12;

Having regard to the Garante's decision No 229 of 8 May 2014, concerning "Determination of simplified arrangements to provide information and obtain consent in connection with the use of cookies" as published in Italy's Official Journal No 126 of 3 June 2014;

Having regard to the Opinion by the Article 29 Working Party (hereinafter, WP29) No 05/2014 on the use of anonymisation techniques as adopted on 10 April 2014 and available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf;

Having regard to the Opinion by the WP29 No 04/2012 on cookie consent exemptions as adopted on 7 June 2012, and to the Working Document by the WP No 02/2013 providing guidance on obtaining consent for cookies as adopted on 2 October 2013, which are available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf and http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf, respectively;

Having regard to the Opinion by the WP29 No 2/2006 on privacy issues related to the provision of email screening services as adopted on 21 February 2006 and available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118_en.pdf;

Having regard to the Opinion by the WP29 No 10/2004 on more harmonized information provisions as adopted on 25 November 2004 and available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf;

Having regard to the records on file;

Having regard to the considerations made by the Office as submitted by the Secretary General pursuant to Article 15 of the Garante's Rules of Procedure No 1/2000 of 28 June 2000;

Acting on the report submitted by Mr. Antonello Soro;

WHEREAS

1. Google Inc. (hereinafter, Google) was founded in September 1998 and is headquartered in Mountain View, USA. The company has about 70 branches and offices in 40 countries worldwide. In Italy, Google set the registered office of its branch called Google Italy S.r.l. more specifically in Milan, by the agency of its subsidiary called Google International LLC. Google Italy S.r.l. is a single-partner company established in 2002 having separate legal personality; partly in pursuance of the "marketing and service agreement" with Google Inc., it deals mainly with promoting, marketing and selling advertising spaces as generated on the www.google.it website and on all the other web pages in Italian that may be traced back in whatsoever manner to the said company. By an instrument of 2010, Google Inc. appointed Google Italy as its representative in Italy for the purposes and under the terms of Section 5 of the *Code* "with regard to application of the Privacy Code and personal data protection legislation."

Google offers a wide array of features to its users ranging from a web search engine (Google Search) to email (Gmail); from online mapping (Street View on Google Maps) to the marketing of advertising space (DoubleClick); from a browser (Google Chrome) to social networking (Google +); from online payment services (Google Wallet) to a virtual store for purchasing apps, music, movies, books and magazines (Google Play); from search, display and posting of videos (YouTube) to text storage, sharing and revision services (Google Docs and Google Drive); from satellite imaging software (Google Earth) to calendar services (Google Calendar); from features enabling management and control of user profiles (Google Dashboard) to statistical analysis and monitoring tools to gauge website visitors (Google Analytics); and so on.

In the vast majority of cases, the above features are offered for free to end-users, since the company's business model is grounded first and foremost in its advertising revenues.

Users may be distinguished, in turn, depending on whether they hold an account that has been created following registration for "authenticated" access to Google's features – these being the so-called "authenticated users" – or else use those features without having first authenticated themselves – these being the so-called "non-authenticated users".

There is actually an additional group of users, i.e. the so-called "passive users"; although they do not use Google's features directly, their data may nevertheless be acquired by the company – for instance, because they are browsing sites of third parties where Google's cookies are installed along with other cookies. This issue will be addressed more specifically below.

On 24 January 2012, Google announced that it would change its privacy policy as from the 1st of March of that year by merging the round 70 policies in place up to then into a single document; each of those policies concerned the provision of a different service. The new rules would therefore apply to all the services offered by the company and to all the different categories of users of such services.

On 2 February 2012, the WP29 informed Google by way of the CNIL (Commission Nationale de l'Informatique et des Libertés), which had been mandated to do so, that it would carry out an inquiry into the new privacy policy in the light of the aforementioned Directive 95/46/EC. The inquiry would specifically target compliance of the data processing performed by the company with the legislation on personal data protection and the free movement of such data.

On 16 March 2012, the CNIL sent Google a questionnaire supplemented later by an Appendix in order for the company to clarify several data processing issues; Google replied to the questionnaire by way of several subsequent communications.

Accordingly, the WP29 sent a letter undersigned by all the Heads of EU's DPAs on 16 October 2012 to notify the company, based on the above inquiries, that its data processing failed to be compliant with the requirements arising out of the applicable EU legislation and to urge the adoption of such measures as were found appropriate to ensure respect for specific principles. The WP29 also resolved to set up an ad-hoc task force made up of some EU's DPAs, including the Italian Garante.

However, Google did not follow up on the recommendations as indicated by the WP29.

By a letter dated 2 April 2013, the Italian Garante notified Google – as the other DPAs in the task force did – that it had initiated an administrative proceeding to check lawfulness and fairness of the processing operations performed by the company under the new privacy policy; the proceeding resulted from specific complaints lodged with the DPA as well as from the findings of the inquiries carried out by the WP29 (via the CNIL).

As part of the said proceeding, the Garante sent several requests for information to Google and held several hearings with the company's representatives, which allowed obtaining multiple – though partial – replies to the questions raised. The deadline for finalizing the proceeding was extended repeatedly, following various stay of proceedings decisions, in order to allow getting all the information required to piece together the many features of the case at issue – partly on account of the specific requests made by the company, which alleged, in the first place, the complexity of the questions raised along with its readiness to bring about changes and implementing arrangements to the processes underlying and determining the mechanisms for processing users' personal data.

In the course of the proceeding, Google adopted various measures and changed its privacy policy to bring the processing of personal data more into line with the applicable legislation. For instance, Google improved the information notice on the use of cookies and other identifiers, on the use of location data or credit card information – compared to what was the case when the WP29's inquiries were started. Examples were added also via pop-up windows; the management of multiple accounts was simplified; the technical terminology was made more understandable by average users; and so on.

Having concluded the fact-finding part of the proceeding, the Garante found nevertheless that, in the light of the provisions made in the Code, the following criticalities still affected the processing of personal data by the company:

A) Mechanisms and contents of the information provided to data subjects as also related to the clarification of the individual purposes and the mechanisms relied upon in processing personal data (see Terms of Service and Privacy Policy, version of 31.03.2014) (Section 13 of the *Code*);

B) Failure to request users' consent for the purpose of profiling them also in order to display customized behavioral ads and to analyse and monitor their navigation; failure to respect data subjects' right to object (Sections 7, 23, 24 and 122 of the *Code*).

The profiling in question and the related serving of targeted ads and/or the analysis and monitoring of users' navigation are carried out basically by

a) Processing, in an automated manner, the personal data relating to authenticated users in connection with the emailing service called Gmail as for both incoming and outgoing email messages;

b) Matching the personal data collected in connection with the provision and use of several features out of those made available to users;

c) Using cookies and other identifiers (authentication credentials, fingerprinting, etc.) as necessary to trace back specific actions or recurring behavioral patterns in the use of the available features to identified or identifiable entities;

C) Retention periods of the personal data (Section 11 of the *Code*).

2. Regarding letter A) in the foregoing paragraph, Section 13 of the *Code* provides that "*The data subject as well as any entity from whom or which personal data are collected shall be preliminarily informed, either orally or in writing, as to: a) the purposes and modalities of the processing for which the data are intended; b) the obligatory or voluntary nature of providing the requested data; c) the consequences if (s)he fails to reply; d) the entities or categories of entity to whom or which the data may be communicated, or who/which may get to know the data in their capacity as data processors or persons in charge of the processing, and the scope of dissemination of said data; e) the rights as per Section 7; f) the identification data concerning the data controller and, where designated, the data controller's representative in the State's territory pursuant to Section 5 and the data processor (…)* ".

The fact-finding part of the proceeding allowed establishing that the information notice as currently available to users, though improved compared to what was the case at the start of this proceeding, is not as yet fully compliant with the aforementioned provisions.

There is little doubt that users must be aware beforehand of the uses their information may be put to; this is a fundamental precondition to enable data subjects to give or refuse their consent to the data processing operations described by the company, having determined directly what impact such processing may produce on their right to the protection of personal data.

The law requires accordingly that the privacy policy made available by Google to provide information to its users should be easily accessible – for instance, it should only be one click away from the user's landing page – and that it should be worded clearly, thoroughly and understandably.

Likewise, it is necessary for data subjects to be in a position to understand and assess any changes or updates made to the privacy policy – possibly by comparing the different versions of that privacy policy over time.

In redrafting its privacy policy, Google may want to follow the recommendations made by the WP29 in its Opinion No 10/2004 on more harmonised information provisions, in particular by adopting a layered notice approach. Indeed, "*Multi-layered notices can help improve the quality of information on data protection received by focusing each layer on the information that the individual needs to understand their position and make decisions. Where communication space/time is limited, multi-layered formats can improve the readability of notices*."

However, it should be pointed out that such a multi-layered format should be configured by preventing fragmentation into an excessively high number of levels – as this would make the information difficult to retrieve and thus undermine its usefulness. Thus, whilst retaining the multi-layered approach to the information notice, the Garante considers it appropriate for the information to be allocated as follows:

- A first or initial layer should accommodate all the information of a general import that is most relevant to users; this

should include, inter alia, what processing of personal data is performed, the personal data or the categories of data being processed (e.g. user terminal equipment location data, wi-fi access points, IP addresses, MAC addresses, financial transactions data, etc.), the fact that the company is the data controller along with the applicable contact information, and the specification of the representative appointed for Italy as well as contact information for users to exercise their rights easily and by using the Italian language.

As for data controllership, it should be emphasized that Google purchased YouTube in October 2006; thus, this specific video sharing feature has become an integral part of the Google domain. Since it was found that Google did not clearly inform users as to its being the controller of the personal data collected also via the service in question – which data is subsequently matched with the information relating to other features – it is necessary that this piece of information is given visibly both in the privacy policy and on the YouTube pages.

This first or initial layer should also include links to the policies applying to the individual features, where existing, and mention – to the very least – the profiling purpose that is pursued by Google also in order to display customised behavioural ads and analyse and monitor users' navigation by way of several mechanisms: processing, in an automated manner, the personal data relating to authenticated users in connection with the emailing service called Gmail as for both incoming and outgoing email messages; matching the personal data collected in connection with the provision and use of several features out of those made available to users; using cookies and other identifiers (authentication credentials, fingerprinting, etc.) as necessary to trace back specific actions or recurring behavioral patterns in the use of the available features to identified or identifiable entities.

Along with specifying the aforementioned profiling purposes and the mechanisms relied upon to achieve those purposes, the first-layer information notice should also spell out how consent to the processing may be given – where necessary. This issue will be addressed below more extensively.

- The second layer may be reserved for the policies relating to the individual features, or for providing examples that clarify how personal data is processed. Currently, such a second layer is already available for specific features (e.g. Google Wallet, Chrome (OS), Books and Fiber), but not for the whole set. This second layer might also be used to store previous releases of the privacy policies, mention the specific risks arising to data subjects from the use of the individual services (e.g. if the selected password is insufficiently secure) and provide such additional details and information as may be appropriate to facilitate the exercise of users' rights.

The rules applying to effective and fair information notices must be the same regardless of the terminal equipment being used (mobile phones, tablets, desktop PCs, portable devices, TV plug-ins, etc.) and of the specific feature made available to users.

3. Regarding letter B) of paragraph 1, one should first of all recall the general principle laid down in Section 23 of the *Code*, whereby "*Processing of personal data by private entities (…) shall only be allowed if the data subject gives his/her express consent*." Additionally, the consent in question is only valid if "*it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information referred to in Section 13*." Section 24 lays down several preconditions that are equated to consent and, if met, allow processing personal data in the absence of consent. They include, by way of example, the need to comply with legal obligations; the fulfilment of contractual obligations; the achievement of a legitimate interest vested in the data controller and/or in a third-party recipient of the data, and so on.

The general scope of this principle is specified in Section 122, which is contained in Title X of the *Code* where electronic communications are regulated (Chapter I – "Electronic Communications Services"); accordingly, "*Storing information, or accessing information that is already stored, in the terminal equipment of a contracting party or user shall only be permitted on condition that the contracting party or user has given his consent after being informed in accordance with the simplified arrangements mentioned in section 13(3). This shall be without prejudice to technical storage or access to stored information where they are aimed exclusively at carrying out the transmission of a communication on an electronic communications network, or insofar as this is strictly necessary to the provider of an information society service that has been explicitly requested by the contracting party or user to provide the said service*."

3.1. If one considers the activities performed specifically in order to provide emailing services via Gmail (see item a) under letter B) of paragraph 1 above) along with the information provided by Google in this respect also during the fact-finding phase of the proceeding, one can draw the conclusion that the company – like all main email service providers – performs the automated processing of the personal data of the authenticated users of the service in question. This processing serves multiple purposes. Some of them, including those that are purely technical in nature, are related directly to the provision of the service at issue according to specific arrangements – e.g. filtering spam; detecting viruses; enabling users to perform text searches, correct spellings, forward messages selectively or provide out-of-office replies automatically, manage preferences and create rules to automatically allocate mail to specific folders based on its contents, or flag urgent messages; enabling the read-out of messages for visually impaired users; converting incoming emails into texting for mobile phones, etc. .

The processing of data subjects' information for the above purposes – which takes place in a fully automated manner, as clarified by the company, i.e. without any human intervention – and/or in order to ensure security of Google's services does not require the data subjects' prior consent as per Directive 95/46/EC, Directive 2002/58/EC and the *Code*. Indeed, the processing in question falls under the scope of the derogation from consent obligations because it is performed to fulfil obligations arising out of the contract for the provision of emailing services.

As regards purposes that go beyond those that are directly and closely related to the provision of specific emailing services, in particular in order to display, to authenticated users, customised ads based on behavioural advertising technology, it is conversely necessary for Google to obtain its users' prior informed consent.

In this connection, reference can also be made to the conclusions reached by the WP29 in its Opinion No 2/2006 on privacy issues related to the provision of email screening services as adopted on 21 February 2006. In addressing the difficult balance to be struck between the protection of privacy in electronic communications and the provision of emailing services whilst pursuing the objective to "*promote technology which incorporates data protection and privacy requirements in the building up of the infrastructure and the information systems including terminal equipment*", the Working Party expressly encouraged the industry to "*devise and develop privacy compliant systems in such a manner as to reduce the processing of personal data to the very minimum; limiting it to what is absolutely necessary and proportionate to achieve the purposes of the processing.*" In this Opinion, the Working Party also tackled the issue of drawing a line (if any) between processing of personal data for service management or network security purposes – which does not require the data subject's prior consent – and the processing that serves further purposes; thus, it was found that if the processing was not grounded in the need for a provider to ensure service security (as per Article 5(1) of the e-privacy directive), the provider was not permitted to carry out any further processing "*without the consent of the users*".

Having outlined the reference legal framework, one can conclude regarding the case at hand that – as already pointed out – Google must obtain the prior informed consent of authenticated users as regards profiling aimed at serving targeted behavioural ads by way of the automated processing of such users' personal data in connection with their use of the emailing services made available through Gmail.

At all events, the Garante reserves the right to take such measures as may be found appropriate in order to safeguard data subjects in connection with the use of emailing services.

3.2. Regarding item b) of letter B) in the foregoing paragraph, it was found that Google matches data subjects' personal data resulting from the use of several features out of those made available by the company. This was actually declared by Google both in a letter sent to CNIL on 20 April 2012 to reply to the questionnaire it had received (see Question 30 therein) and in its privacy policy as last amended on 31.03.2014 ("How we use information we collect"). The rationale of this specific processing is the following according to Google: "*We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads.*

We may combine personal information from one service with information, including personal information, from other Google services." [1]

The above conduct is in line with the company's business logic, since Google has repeatedly stated that it seeks to provide its users with a unified service by way of the integration and interoperability of several products and features – also in order to improve user experience regarding those features (see letter sent by Google to the Garante on 6 December 2013). However, this is not in line with what is required by the law, since the processing performed to profile users also with a view to analysing and monitoring user navigation as well as to send targeted ads by matching, inter alia, data collected in connection with multiple features does not fall under the scope of any of the consent exemption cases mentioned in Section 24 of the *Code*. Accordingly, such processing may only be performed with the user's prior unambiguous consent.

Nor is it enough for the above purpose to be mentioned in the information notice to data subjects, as this does not exempt Google from the obligation to obtain the data subjects' consent in this respect. It should be considered that the privacy policy currently available on Google's websites contains the following statement: "*We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy*." Such a statement would appear to imply exactly that all the processing operations serving purposes that are mentioned in the Privacy Policy do not need the user's prior express consent as given by way of an affirmative action signifying his or her intentions.

As it may be expected, the Garante does not concur with this conclusion; in fact, the Garante holds the view that the processing in question should be regulated differently in accordance with different arrangements.

3.3. Regarding Google's activities as mentioned under item c) in letter B) of paragraph 1 (use of cookies and other identifiers such as authentication credentials, fingerprinting, etc.), it should be pointed out that Google's privacy policy only contains the following statement: "*We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services*." This is similar to what was found with regard to profiling as performed via matching and combination of data.

In the course of the fact-finding activity, it could be established that Google had made available a specific information notice to users (in April 2013) regarding installation of cookies on their terminal equipment. The notice reads as follows: "*Cookies help us provide our services. Using these services, you accept our use of cookies*." The notice includes a so-called "OK button" users may click to only inform Google that they have seen the above notice. That is to say, clicking this button is in no way instrumental to enabling the data subject to make an informed choice, since the cookies are installed in any case on the data subject's terminal equipment irrespective of whether the OK button is clicked or not.

Furthermore, it is in no way envisaged that the data subject's consent be obtained prior to storing such identifiers on the respective terminal equipment – or rather, this consent is surmised through implication in accordance with the statement contained in the above summary information notice by relying on the user's passive acceptance of the terms of use and on the user's "further browsing", i.e. on the fact that the user continues navigating the website. Additionally, it was found that no tools are made available to allow data subjects to object to the processing in question.

As for the use of identifiers other than cookies, which are mentioned in the privacy policy, it would appear that no mechanisms have been implemented to allow users to minimally voice their wishes in this respect: indeed, the aforementioned "OK button" only refers expressly to cookies.

It should be pointed out in this connection that identification based on tools other than cookies relies on the processing by Google of personal data and/or information or pieces of information that is not yet personal data (but may become so if matched or combined with other pieces of information) in order to single out the terminal equipment and, in this manner, the profile of one or more users of such equipment. This is the so-called fingerprinting and is used by Google for the selfsame profiling purposes also with a view to displaying targeted ads and analysing and monitoring users' navigation; as is the case with the use of cookies, fingerprinting is regulated by Section 122 of the *Code* and is accordingly conditional upon obtaining the data subject's prior consent except for the cases referred to in the law – here, the conveyance of a communication on an electronic communications network or the provision of a service upon the user's request.

There is a difference between using cookies and fingerprinting, which the Garante would like to emphasize. In the former case, users who do not wish to be profiled may apply the legal remedy consisting in their right to object to the processing but may also apply the pragmatic remedy consisting in removing the cookies stored on their terminal equipment. In the case of fingerprinting, the only remedy available to users consists in making a specific request to the data controller and hoping that such request is granted. This is due to the fact that the fingerprint does not sit in the user's terminal, as it is actually stored in the provider's systems which are obviously out of the user's reach.

Based on the above considerations, it is unquestionable that the processing arrangements implemented by the company for profiling purposes also with a view to displaying targeted ads and analysing and monitoring users' navigation do not meet the requirements set forth in Sections 23, 24 and 122 of the *Code*. Accordingly, it is necessary for such arrangements to be amended as well.

In other words, the processing at issue may only be carried out with the data subject's prior consent; this consent must be compliant with legal requirements in order to be valid: thus, it must be free; it must be obtained prior to starting the processing; it must apply to processing operations for explicit and specific purposes; it must be informed; and there must be written proof of such consent.

From this standpoint, it is necessary for consent to be given in such a way as to unambiguously signify the data subject's intention.

4. Freedom of enterprise as well as the fact that Google is the data controller and is accordingly empowered to "*determine (…) methods of the processing of personal data*" (under Section 4(1), letter f), of the *Code*) leave no doubt as to Google's discretion in selecting the standards and measures to ensure that the processing of users' data for profiling purposes (whatever the relevant mechanisms) is compliant with the law.

Nevertheless, taking account of the specificities of the online services offered by the company, the Garante is proposing a solution that can meet the applicable requirements as set forth, in particular, in Sections 7, 23 and 122 of the *Code*.

Against this backdrop, it can be safely assumed that there must be a phase or moment, during the user's navigation experience, when he or she should be enabled to make a choice out of several options – needless to say, prior to using any of the features made available by the company.

On the other hand, given the distinction to be drawn between authenticated and non-authenticated users as explained in the foregoing paragraphs, the mechanisms to obtain consent may vary exactly with the specific user category.

4.1. Regarding non-authenticated users, it was found that there is as yet no physical or virtual room at any time or in any phase of their use of one or more features such as, on the one hand, to enable them to consent to the processing as described

above and, on the other hand, to enable Google to take note and keep track of the choice made by such users.

Given the above, it is necessary for Google to implement the mechanism in question – for instance by making sure that a non-authenticated user accessing the home page or any other page of Google's websites is immediately displayed a suitably sized (overlay) area such as to give rise to a perceptible disruption in the user's experience of the web page being visited. The area at issue should include at least the following:

> i) Information to the effect that the website processes data for profiling purposes by way of the automated processing of personal data relating to authenticated users as regards the emailing services provided via Gmail, by way of the matching and combination of data from different features and by way of cookies or other identifiers also in order to send online targeted ads pursuant to the preferences shown by users availing themselves of the Net-based features and browsing as well as in order to analyse and monitor users' navigation behavior;
>
> ii) a link to the privacy policy providing all the information mentioned in paragraph 2);
>
> iii) a link to a separate dedicated area where users may refuse to consent to profiling or else select, out of an exhaustive set of options, the feature(s) and mechanisms in whose respect they accept to be profiled;
>
> iv) information to the effect that if the user continues browsing by accessing or selecting an item below and/or outside the said (overlay) area (e.g. a search form, a map, a picture, a link, and so on), he or she consents to profiling.

The area in question must be an integral part of a mechanism that enables an affirmative action such as to signify the data subject's consent. In other words, it should be disruptive – albeit minimally – of the user's navigation experience: to overcome or skip the on-screen display of the (overlay) area, the user must take specific steps, i.e. he or she must select an item that is part of the page underneath the said area.

Furthermore, there is little doubt that - legally and technically speaking - the action consisting in accessing the dedicated "fine-tuning" area or clicking the ad-hoc privacy policy link may not be construed in the manner described in the foregoing paragraph.

It should be pointed out that each of the actions left to the user's discretion generates a specific IT event, which can be recognised unambiguously by the service provider so that the latter can easily keep track of it.

If a user consented that their data would be used for the purposes specified, the above mechanism is fully in line with the requirements made in Section 23 of the *Code* - whereby "*written proof*" of consent is necessary.

The availability of this "proof" that consent was obtained from the data subject will allow Google to not introduce any additional disruption in the user's experience upon subsequent visits to the domains covered by this decision, if such visits are performed via the same terminal equipment. This is without prejudice to the possibility for the user to refuse consent and/or change their mind at any time and in a user-friendly manner (see Section 7(4) of the *Code*). Indeed, it is exactly with a view to effectively exercising this self-determination right that all the web pages targeted by this decision should contain a link to the dedicated area where users may exercise their rights thoroughly.

Conversely, if a user only clicks the link to the privacy policy in order to get additional information for making more informed choices, the mechanism described above should set in immediately the user takes a step after viewing the said information notice so as to enable him or her to give or refuse their consent to the processing.

If a user accesses the fine-tuning area, Google will have to log this action – which may not be equated to consent, as already specified, exactly like the user's clicking the privacy policy link – and pool this information with the additional indications coming from the specific options selected by the user also in a detailed manner.

In order to keep track of the actions and (detailed) options left to the data subject's discretion – in particular, the fact of giving his/her consent to profiling, in whole or in part, as well as his/her exercise of the right to object to profiling – Google might rely either on ad-hoc technical cookies (see also Recital 25 in Directive 2002/58/EC) or on identifiers other than cookies.

A further caveat should be considered if the aforementioned "proof" of consent is based on the use of cookies – namely, if a user decides (as all users are empowered to do) to delete all the cookies installed on his/her terminal equipment including the said "technical" cookie, this action does not equate to the exercise of the user's right to object as it does not entail any interaction with the data controller. Accordingly, Google should re-activate the consent acquisition mechanism described above also in such a case.

Conversely, if Google decided to rely on identifiers other than cookies, which are therefore stored outside the user's terminal equipment since they sit in the servers owned by Google, it must not re-activate the consent acquisition mechanism (i.e. no new disruption of the user's experience will be necessary) in case the user's preferences are modified;

thus, Google will only have to update those preferences as already stored in its servers.

4.2. The mechanism described above is meant to create a physical or virtual area for obtaining and managing consent from non-authenticated users.

It is unquestionable that authenticated users must also be afforded the same protection; furthermore, it is appropriate that whoever holds a Google account should be in a positon to rely on the consent acquisition/withdrawal/refusal mechanism described in the foregoing paragraphs for non-authenticated users so as to ensure that the same user experience is available throughout. The main difference between the two categories of users consists in the extent to which the choice made may be traced back to a given user directly or indirectly – since an authenticated user is in a sense identified *per se*.

Additionally, one should consider that authenticated users – whether they are about to create a new account or already hold an account and plan to access a log-in session to authenticate themselves and use the relevant features – are bound to go through a phase when they are as yet unknown to the system, exactly because they have yet to create an account or authenticate themselves in order to use specific features. It is therefore appropriate that in this "preliminary" phase they are offered the same consent acquisition mechanism as non-authenticated users – the only difference being that if they accept to continue browsing and thus give their consent by overcoming or skipping the disruption introduced in the manner described above, so as to land either on the account creation page (new authenticated users) or on the log-in page (Google account holders), no additional cumbersome requirements should be envisaged for this "preliminary" phase. It is actually in this phase that the system can directly and unambiguously allocate specific behaviors and decisions to specific entities.

In line with the purpose limitation principle as regulated in the *Code*, the Garante's view is accordingly that – under the given circumstances – the subsequent step described above is to be regarded as a specification of the foregoing phase and can be managed by prioritizing the informed choice already made by the non-authenticated user; that is to say, the choice made beforehand can be considered to hold true also at the time (which is both logically and chronologically subsequent) when the status of that user changes in that he or she turns into an authenticated user. However, this is strictly conditional upon a two-fold requirement : on the one hand, the user must be informed thoroughly of the mechanism (described above) to confirm his/her choices as already made in his/her capacity as a non-authenticated user along with the circumstance that some features are only available to authenticated users and the relevant choices may only be made accordingly by such users; on the other hand, the user must be in a position to at any time change his/her mind (by withdrawing his/her consent or overcoming his/her refusal to consent) and add to his/her choices by having regard to the features that are only available to authenticated users (e.g. Gmail). To that end, an ad-hoc link to the dedicated area must be displayed prominently in order for users to exercise the said rights, which may also take place by way of exhaustive, detailed options; this means that the area in question should also include the list of the features that may only be operated by authenticated users, who are therefore the only ones enabled to make the relevant decisions.

It shall be understood that the decisions made by a non-authenticated user with regard to processing of one's own data for profiling purposes may only apply to the specific device/equipment being used – exactly because they do not relate to a specific account; this is so both in the initial and in the subsequent sessions until those decisions are revoked. The matter stands differently in the case of authenticated users: indeed, the decisions made by such users cannot but hold true also if they use the available features and services by relying on different devices – exactly because those decisions can be traced back directly to an individual that is identified and identifiable *per se*.

In other words, proof of the consent given by a non-authenticated user only applies to the given device/equipment being used, whilst proof of the consent given by a Google account holder is valid regardless of the device/equipment being used.

Finally, as regards passive users – i.e., any entity that does not use Google's features directly but whose data may be acquired by the company, for instance because they are visiting websites of third parties other than Google where Google's cookies are also hosted – the Garante refers expressly to the measures mentioned in its decision No 229 of 8 May 2014 concerning "*Determination of simplified arrangements to provide information and obtain consent in connection with the use of cookies*" (published in Italy's Official Journal No 126 of 3 June 2014). In that decision it is provided a) that it will be up to the publisher, i.e. the entity managing the website being visited, to obtain consent in such a case also with a view to the storage of cookies by Google, and b) that the said publisher should also obtain the links to the web page(s) containing the relevant information notices and the consent provision forms relating to Google's cookies at the time of entering into the respective contractual agreements.

Whilst reiterating that Google has full discretion in selecting the technical arrangements it considers to be most appropriate in order to ensure that its processing of personal data is compliant with the applicable legislation, the Garante believes that the mechanism described in the foregoing paragraphs is the least disruptive one in terms of user experience given the current status of Internet technology.

5. Regarding letter C) in paragraph 1 on data retention periods, it should be recalled that Section 11(1), letter e), of the *Code* provides that the data must be "*kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed*."

In its letters of 16 and 22 May 2012, the WP29 requested the company to clarify for how long users' data were kept and, in particular, the maximum retention periods of such data with regard to the purposes of the individual data processing operations. This issue was also addressed subsequently in the course of the national proceeding; the Garante requested Google to provide additional information to that contained in its replies to the WP29, but it did not receive exhaustive clarification.

In fact, in its letter of 28 June 2013, Google recalled what it had already stated with regard to the storage period of the so-called "search history" – namely, that the data were stored for an indefinite amount of time or until the user removed them from his web history (as for non-authenticated users) or for up to 180 days (in the case of authenticated users), and that the storage period was 9 months for non-anonymised IP-addresses and 18 months for cookies. For the remainder, and still by way of example, Google referred to the "instant service" search strings of Google Search, which were said to be deleted "usually after two weeks" (see replies to questions 19 and 20). Nor did one find it especially helpful what could be read in the online help page for Google accounts as of the time when it was accessed during the inquiries carried out by the Office – whereby users can delete web history data by way of the "delete" feature. In this manner, so it read, the data will be deleted from the service. "*However, Google keeps a separate log system for supervision and to improve the quality of our services*." (see https://support.google.com/accounts/answer/54052?hl=it). This passage was actually slightly modified during the course of this proceeding, so that it reads as follows currently: "*When you delete items from your Search History, they are no longer associated with your Google Account. However, Google may store searches in a separate logs system to prevent spam and abuse and to improve our services.*"

Two main considerations should be made in this regard. Firstly, it would not appear to be enough for Google to state that a user's web history is no longer associated with that user's account if it then fails to clarify whether this can actually ensure the effective anonymisation of the relevant data pursuant to the standards and principles set out by the WP29 in its Opinion No 05/2014 on the use of anonymisation techniques (as adopted on 10 April 2014).[2]

Secondly, there continues to be a vague statement to the effect that the personal information in question remains available to Google even after its deletion for reasons allegedly related to improving Google's services – for a potentially unlimited period.

Thus, in spite of the amendments made to the text of the said privacy policy, this Authority considers that the said policy is not compliant with the lawfulness of processing requirement set forth in the *Code* as also related to this feature. Accordingly, it would appear to be necessary for Google to implement new, more stringent safeguards for data subjects in this respect.

In this connection, it should be pointed out that respect for data retention and storage principles may be ensured by way of two main mechanisms – i.e. either by ensuring compliance with the purpose limitation principle, whereby no data may be kept for longer than is necessary to achieve the purpose for which such data was processed (i.e. by way of a retention policy) or else by having regard to the decision (and the subsequent affirmative action, or the request) made by a data subject to have Google delete, under certain conditions, the personal data relating to him/her (i.e. by way of a deletion policy).

Based on the system implemented by Google, the information at issue is stored as a function of the time elapsed from when it was first collected. One can actually draw a distinction between data that is stored in the so-called active systems (live-serving systems) and the data that is stored subsequently in back-up systems. Furthermore, it should be highlighted that it was not possible to clarify in the course of the fact-finding activities for how long data is stored in the former systems and therefore when such data starts being stored in back-up systems. Nor did the company clarify what was the maximum retention period of data subjects' personal information.

The deletion of personal data held by Google was recently addressed by the well-known judgment of the Court of Justice of the EU dated 13 May 2014 (case C-131/12). The Court ruled, inter alia, exactly on the deletion of data contained in Google Search results in case the preconditions for exercising one's right to be forgotten are fulfilled; the Court found in this regard, for the first time, that such deletion requests may be also addressed directly to the search engine even though the relevant information was published originally on other websites and was subsequently indexed by Google.

The above ruling by the CJEU in this highly complex as well as sensitive area along with its multifarious, highly significant implications – including those on the measures to be taken to handle the deletion requests at issue – were the subject of an initial analysis also by the WP29. In the course of its plenary meeting held on 2 and 3 June 2014, the WP29 resolved to investigate the consequences of the said judgment and "*identify guidelines in order to develop a common approach of EU data protection authorities on the implementation of the ruling. These guidelines will help data protection authorities building a coordinated response to complaints of data subjects if search engines do not erase their content whose removal has been requested*." (see Press Release of the WP29 of 6 June 2014, available at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140606_wp29_press_release_google_judgment_en.pdf.)

At all events, Google has made available a tool since 30 May 2014 to enable users to lodge the respective deletion requests pursuant to the ruling of the CJEU. This tool was welcomed by the WP29, which declared in this connection that it represented "*a first step toward compliance with EU law following the CJEU ruling, even if at this stage it is too early to comment on whether the form is entirely satisfactory*." (see aforementioned Press Release).

The peculiarly innovative features of this subject matter and the complex implications entailed by fulfilment of the CJEU's ruling as for the requests to delete one's personal data in Google Search results - in case the preconditions for exercising one's right to be forgotten are met - would appear to point to the advisability for the Garante to refrain, at this stage, from requiring Google to implement measures that have yet to be tested in the field and do not reflect a common approach as devised by all the DPAs concerned by the ruling in question. This is also in line with the statements made by the WP29 as reported above.

In the light of the foregoing considerations and without prejudice to such measures as may be deemed appropriate to afford the widest possible scope of protection to users' rights in line with the said preliminary ruling by the CJEU, the Garante will limit itself, at this stage, to issuing specific instructions with regard to data deletion requests lodged by authenticated users, i.e. by users holding Google accounts. Indeed, such deletion requests enable the company to unambiguously identify the applicants as well as the specific items of information to be possibly deleted – as such information can be automatically traced back to the applicant's account and no discretionary appreciation is necessary in this respect.

Furthermore, taking account of the foregoing considerations regarding the CJEU's ruling, the Garante will limit the scope of application of this decision to data deletion requests that concern features other than Google Search – as the right to be forgotten may be exercised with regard to the latter if certain preconditions are met.

Accordingly, based on the fact-finding activities mentioned above, the Garante holds the view that Google is required to develop a data deletion policy regarding data deletion requests made by authenticated users; this is meant to ensure that the processing of data performed by the company as described above is in line with the law. The policy in question must comply with the provisions set forth in the operative part of this decision. Additionally, Google is required to develop a data retention policy that takes utmost account of the need to comply with the purpose limitation principle laid down in Section 11(1), letter e), of the *Code*.

6. The Garante is aware of the technical and operational difficulties arising from implementation of the measures Google is required to take in order to comply with the provisions made herein. Indeed, the measures in question relate to multifarious features that are made available on the most diverse technological platforms and operating systems and entail far from negligible technicalities. Given the above, one can assume that the time range for compliance needs to be sufficiently wide and can be set at 18 months. During this period, the Garante reserves the right to assess the progress made in implementing the measures as well as compliance with the operational plan for their development and implementation – to be submitted by Google. In this perspective and in the light of the specific proposal put forward by the company in the course of the fact-finding activities, the Garante will accept Google's binding, irrevocable undertaking to undersign an ad-hoc verification protocol. Such protocol is meant to regulate the mechanisms and time schedule for the exchange of documents between Google and the Garante as well as the arrangements for the enforcement and oversight activities the Garante will perform in the course of the said period, also at Google's own premises.

BASED ON THE ABOVE PREMISES, THE GARANTE

Taking account of the complex features highlighted by the assessment of Google's new privacy policy in order to establish whether the data processing performed by the company is compliant with personal data processing legislation and whilst expressly reserving the right to carry out more in-depth evaluations and/or make additional decisions if they prove necessary, hereby provides under the terms of Section 143(1), letter b), and Section 154(1), letter c), of the *Code* that Google Inc., having its registered office in Mountain View, USA, should take the following measures as regards specifically the processing of personal data relating to use of the features offered by way of the www.google.it website and of all the other web pages in Italian that may be traced back to the company:

1) Pursuant to Section 13 of the *Code*, thorough as well as effective information notices shall be provided to users in accordance with the criteria and arrangements set out in paragraph 2 hereof;

2) Pursuant to Sections 23 and 122 of the *Code*, the prior consent of both authenticated and non-authenticated users shall be obtained as regards the processing of information relating to them - including processing of the information arising from the automated processing of authenticated users' personal data with regard to the use of the emailing service provided via Gmail, by way of the matching and combination of the personal data collected in connection with the provision and use of whatever features out of those offered to users, and as regards the use of cookies and other identifiers for profiling purposes, also with a view to serving behavioural ads and analyzing and monitoring users' navigation. This shall be done in accordance with the criteria and arrangements set out in paragraph 3 hereof; furthermore, the data subjects in question shall be enabled to exercise their right to object under Section 7 of the *Code*;

3) Pursuant to the principle set forth in Section 11 of the *Code* regarding data retention and apart from the deletion requests relating to the exercise of the right to be forgotten as made in respect of web search results obtained via the specific search engine feature called Google Search:

a. As for the information stored in so-called active systems, the data deletion requests made by authenticated data subjects shall be complied with by no later than two months; the latter period is considered to be appropriate by having regard on the one hand to the possible non-specific nature of such requests and, on the other hand, to the circumstance that the company can establish the requesting individual's identity and determine, with ease, the specific information covered by the said requests since such information is automatically related to the individual's account and does not leave any margin for appreciation. The said two-month deadline includes 62 calendar days so that the requests in question must be granted prior to the expiry of the 63rd day whilst the relevant data should be deactivated over the initial 30 days. The latter grace period is considered to be necessary to protect the data subject against accidental or fraudulent deletion of their personal data;

b. As for the information stored in so-called back-up systems, deletion shall be effected by no later than six months as from the date of the request made by authenticated users. The latter period includes 180 calendar days, so that the said requests must be granted prior to the expiry of the 181st day; however, during the period in question the only processing operation allowed in respect of the relevant data shall be the recovery of lost information whilst the information must be protected against unauthorised access by means of suitable encryption techniques or, where necessary, by anonymizing the data in question. This should be in line with the principles set forth by the WP29 in its Opinion No 05/2014 on the use of anonymization techniques of 10 April 2014;

c. A data retention policy should be adopted in line with the purpose limitation principle laid down in the *Code*.

4) The measures mentioned under paragraphs 1 to 3 above shall be implemented by no later than 18 months as from service of this decision.

5) Google shall submit a draft verification protocol to the Garante by 30 September 2014 as specified in the Premises in order for the Garante to evaluate such draft and approve it. The protocol in question shall regulate the verifications and controls referred to therein in accordance with the arrangements and timeline to be specified in the protocol itself. The activities in question shall be carried out over at least 12 months as from approval of the protocol by the Garante.

This decision may be challenged under the terms of Section 152 in the *Code* and Section 10 of legislative decree No 150/2011 by lodging an appeal with judicial authorities by no later than thirty days as from the date of service; the latter deadline shall be sixty days if the appellant party is resident abroad.

Done in Rome, this 10th day of the month of July 2014

THE PRESIDENT
Soro

THE RAPPORTEUR
Soro

THE SECRETARY GENERAL
Busia

---

1) In a paper recently published by Hal R. Varian, chief economist at Google, titled "Beyond Big Data", which was presented on 10 September 2013 at the NABE Annual Meeting in San Francisco, CA, the following can be read: "Google runs about 10,000 experiments a year in search and ads. There are about 1,000 running at any one time, and when you access Google you are in dozens of experiments. What types of experiments? There are many: user interface experiments, ranking algorithms for search and ads, feature experiments, product design, tuning experiments" (see http://people.ischool.berkeley.edu/hal/Papers/2013/BeyondBigDataPaperFINAL.pdf). This statement captures a phenomenon that has huge proportions and is markedly integrated within Google's business logic; nevertheless, it is often unknown to users and – most importantly – users are unable to exercise their self-determination in this respect.

2) It is widely known in sector-specific literature that removing directly identifying information does not prevent, especially in online services, the subsequent re-identification of data subjects. This was shown most clearly in the AOL and Netflix cases (see Opinion No. 05/2014 of the WP29 on the use of anonymisation techniques, adopted on 10 April 2014, paragraphs 2.2.3, 3.1.1.3 and Annex A.2, where additional references can be found in footnotes).