## Appendix: List of possible compliance measures

**Note:**

In order to guide Google in the implementation of the legal requirements regarding data protection, the Article 29 Working Party prepared a common list of requirements and possible measures that Google could implement.

The recommendations are provided for illustrative purposes only and may not be the only means by which Google could achieve compliance. They should be regarded as potential solutions in order to give practical suggestions as to how the requirements could be fulfilled. They do not pre-empt enforcement actions by national authorities based on national law.

Information

1. The privacy policy must be immediately visible and accessible, for instance visible without scrolling and accessible via one click, from each service landing page.

2. To ensure that the information is accurate and comprehensive, the privacy policy must have, at least, the following characteristics:
    a. The privacy policy is structured so as to provide clear, unambiguous and comprehensive information regarding the data processing.

    b. It provides an exhaustive list of the types of personal data processed by Google.

    c. It provides an exhaustive list of all the purposes for which personal data are processed by Google.

    d. It provides information about the identity of the data controller and gives an address so that individuals can exercise their rights. This specifically includes the obligation to clearly identify Google as data controller on the YouTube service.

    e. Google should enable users to have, on a single page, a comprehensive picture of the personal data processed by Google and for which purposes.

3. Users cannot be expected to read the Terms of Service update to be made aware of important new purposes for the collection, processing sharing or any other use of their personal data. Such purposes must be presented in the privacy policy.

4. When Google allows new entities to collect data, it must clearly inform users about the new recipients and the data they are allowed to collect. For instance, Google recently added “and our partners” to the set of entities that may collect anonymous identifiers

when users visit Google services. However, Google did not inform about what type of entities these partners are and how they will use the collected data.

5. Passive users must be better informed about and, if this is the case, allowed to consent to the processing of their personal data:
    a. For Google Analytics, several options can be considered:

        - Google could modify the JavaScript tag so it will inform users and ask for consent depending on the country. Google could also provide an option for users to disable Google analytics on a temporary or permanent site basis. Google could also set the default of the tracking code such that it disables tracking for as long as consent has not been granted.[1]
        - Google could require sites using Google Analytics to display appropriate information regarding the presence of the service and to obtain prior consent. Google could then enforce such a measure. For instance, Google could crawl websites listed as using its analytics solution to verify that an appropriate consent solution is in place.
        - Google could extend the settlement reached in Germany to other countries, such that data are not combined or used for other purposes, even for the improvement of Google Analytics.

    b. For DoubleClick

        - Google could choose to either inform individuals through the JavaScript or enforce its policy through auditing of third-party websites. For instance, if third party websites that use DoubleClick do not inform users about the processing, Google could enforce against these third parties to ensure compliance with the DoubleClick terms of use or by terminating the service.

    c. Google could apply the recommendations for Google Analytics and DoubleClick to all services that are used by passive users.

6. Google should avoid indistinct language such as "we can" / "we may …", but rather say "if you use services A and B, we will …".

7. Google's internal policies should provide clear guidance to Google employees that new services and features based on the collection of new data or processing for new

[1] An example of such code is provided by the CNIL at: http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/outils-et-codes-sources/la-mesure-daudience/ or https://github.com/CNILlab/Cookie-consent_Google-Analytics/blob/master/Tag_google_analytics.js

purposes (i.e. data collected by search nearby and caller ID) require prior user consent (opt-in).

8. Information principles should be applied equally to every terminal type (mobile, tablet, desktop, wearable and other devices such as the Chromecast and Nest) and every client application. If the terminal does not have a suitable end user interface for such information (e.g. Nest), it could be made available on a terminal used to configure it.

9. Google could present the privacy policy using a multi layered approach.
    a. In that case the first layer should describe the general policy with enhanced information and links to service specific policies (where appropriate). The additional information on this layer should at least concern data combination for Google's major services (Gmail, Search, Google+, YouTube, DoubleClick and Google Analytics) and where the combination of data would be reasonably unexpected. The first layer could also provide more information on some categories of data (e.g. location, financial data, unique device identifier and telephony) and has to be presented in a clear, comprehensible and efficient manner.

    b. The second layer could be a service specific policy or further examples to explain how information is processed – this layer does exist for selected services.

    c. The third layer could comprise the "in product notice". Google could continue to develop, expand and improve those "in product notices" to alert users to Google's own data processing purposes.

10. The concept of a personalized privacy policy could be an additional means that could be used to better inform authenticated users, showing only the data processing which Google is conducting with that user's data. For example, for a user of Google Search, Gmail and Google Display Network it would be possible to present only information about those services in a dedicated tool demonstrating how the user's data are combined to deliver these services. This personalized privacy policy could be extended to all users (including passive, active and authenticated) based on cookie information or other credentials already used by Google to identify users. Information would still need to be available for users who are not yet users of a particular Google service and wish to learn more.

User controls

In order to better enable all users (authenticated, non-authenticated and passive users) to control the use of their personal data, Google must provide users with more elaborate tools to manage their personal data and to control the usage of their personal data between all Google services. This could be done by making the current dashboard more accessible (e.g. putting a link in the Google Profile popup) and to include all of Google services. For example, it could be done in the following ways:

1. Through this dashboard, users would be capable to object or consent, where applicable, to data collection and/or combination by any specific services. The deletion of user data and/or removal of services should be made easily accessible.

2. Google could configure the default settings to be specific to each product/service with privacy-friendly defaults (also including regional variations). A feature to "restore to default settings" could also be added to the dashboard.

3. Google could combine all privacy and user control tools into the Dashboard for authenticated users, but also incorporate tools for passive and unauthenticated users into this single repository (e.g. the existing Ads Settings functionality). Currently, the dashboard is only available for authenticated users but it would be possible to extend it (where appropriate) to passive and unauthenticated users with the same means Google already uses to identify these users (e.g. cookies stored in the browser). A link to this dashboard for passive users could be provided in the Privacy Policy of partner websites or through consent mechanisms and information provided to such users. Where tools cannot be included into the Dashboard, appropriate information on how users can access this data should be provided.

4. Prior to processing data for any specific purposes, including the combining of data across services for marketing, product development, personalisation without the user's direct knowledge and analytical purposes, based on identifiers (such as cookies, login credentials, as well as fingerprinting or other identifiers) set through first or third party websites, Google must obtain user consent. In its opinion on consent (Opinion 15/2011 on the definition of consent) and in other opinions (Opinion 2/2010/ WP171 on online behavioural advertising and Opinion 15/2011 on the definition of consent/ WP187 ) the Working Party has clarified the requirements for unambiguous consent as a legal ground for the personal data processing and its main elements:

    a. Specific and information based consent. To be valid, consent must be specific and based on appropriate information. All users of Google services are to be informed in a clear and distinct manner, for instance by means of a pop-up or banner. This banner or area should contain a simplified information notice mentioning the purpose plus a link to Google's privacy policy, as well as an additional link to another area or section where users'

choices can be fine-tuned (to refuse consent to specific purpose, or to select the scope of purpose allowed for by the user with regard to the individual features offered by Google)

b. Timing. Consent has to be given before the processing starts, i.e. before the user can start using the relevant Google service.

c. Active choice. Consent must be unambiguous. Therefore the procedure to seek and to give consent must leave no doubt as to the data subject's intention. There must be an effective and easy way to find mechanism for users to revoke their consent.

d. Freely given. Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.

e. The action performed by the user could generate a specific technical event that could be recognized unambiguously by the service provider, who can therefore keep a log of such events.

f. The choice made by a non-authenticated user is only valid for the given device used for accessing the specific Google features, whilst the choice made by an authenticated user (i.e. a user holding a Google account) is valid irrespective of the device used from time to time.

5. Google could use different cookies (or other identifiers) for different services to enable users to exercise greater control.

6. Prior to the storage of, or access to information on the user's terminal device (e.g. cookies as well as fingerprinting or other identifiers) through first or third party websites, Google must obtain user consent. Practical guidelines on how to comply with the provisions of article 5(3) of the amended ePrivacy Directive 2002/58/EC are provided by Article 29 Working Party in the 'Working Document 02/2013 providing guidance on obtaining consent for cookies' (WP208). The same mechanism that is used to obtain consent for processing (c.f. 4.) could be used to obtain consent in the meaning of article 5(3) of the ePrivacy Directive.

<u>Data Retention policy</u>

1. Google should define retention policies for all personal data processed by Google (collected, generated, produced) about active and passive users. Retention policies should be sent to European DPAs; the retention period for each type of data should be justified and should be specific to each purpose and legal basis.

2. Clarification could be given on the personal data processings which apply to a profile based on an identifier that has not been used for a defined period. Data retention periods associated to such information could be clarified. Data retention must comply with the proportionality principle

3. If Google anonymises data (as suggested in the data retention policy update), it could either disclose the anonymisation process or assess that its process follows the recommendations made in the Article 29 Working Party Opinion 5/2014 on anonymisation techniques.