Decision No […] of […] giving formal notice […]

(No […])

The President of the National Commission for Computing and Liberties,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to the protection of personal data and the free movement of such data, in particular Articles 56 and 60;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 20;

Considering the decree n° 2019-536 of May 29, 2019 taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms;

Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Computing and Liberties;

Having regard to the decision […] of the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or to have carried out a verification mission of any processing accessible from the domain "[…]" or bearing on personal data collected from the latter;

Having regard to referral No. …;

Having regard to the other documents in the file;

I. The procedure

The company […] (hereinafter "the company" or "[…]"), whose registered office is located […], was created in […] and has a distance selling activity.

The National Commission for Computing and Liberties (hereinafter "CNIL") was seized, on August 19, 2020, of a complaint (n° ...) relating to the transfer of personal data of the complainant, represented by the association NOYB - European Center for Digital Rights, to the United States of America, collected during his visit to the website […]. 101 complaints have also been filed by NOYB in the 27 Member States of the European Union and the three other States of the European Economic Area (EEA) against 101 data controllers who would transfer personal data to the States

United.

Pursuant to the decision […] of the President of the CNIL, a delegation from the CNIL carried out a control mission on documents by sending the company […] a questionnaire […] and a request for additional information […]. The company responded by letter […]. Those

questionnaires concerned the transfer of data from visitors to the French version of the website […] which integrates the Google Analytics functionality.

On […], the company informed the CNIL that it had taken the decision to integrate the Google Analytics functionality on its website […] and that the statistics obtained via Google Analytics concerned people in several Member States of the 'European Union. The processing resulting from the integration of the Google Analytics functionality on its website therefore appears to be cross-border within the meaning of Article 4.23.b) of the GDPR.

[…]

In accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter "GDPR" or "the Regulation"), the CNIL informed, […] all European supervisory authorities of its competence to act as lead supervisory authority concerning this cross-border processing implemented by the company, competence derived by the CNIL from the fact that the main establishment of the company is located in France.

[…] authorities are considered to be concerned within the meaning of Article 4, point 22 of the GDPR: the authorities […].

On January 4, 2022, as part of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR.

This project did not give rise to relevant and reasoned objections.

II. On the processing in question and the responsibility for processing

It emerges from the answers of […] sent to the delegation of control that the company has integrated the Google Analytics functionality on the website […] for the purpose of measuring the audience and the performance of the company's media campaigns. The company clarified that Google Analytics made it possible in particular, when the user had not refused its use, to carry out a measurement for tracking the individual. Indeed, by associating the unique identifier of a user with the data of this user coming from one or more sessions launched from one or more devices, Google Analytics makes it possible to obtain a more precise count of users (by identifying a user as a separate user, even in a different session).

[…]

Google Analytics works by including a block of JavaScript code on the pages of a website. When a site user visits a page, this JavaScript code causes a JavaScript file to load and then performs tracking for Google Analytics.
The tracking operation consists of retrieving data relating to the request through various means and sending this information to the Google Analytics servers.

Website managers who integrate the Google Analytics functionality can transmit instructions to Google for the processing of data collected via Google Analytics. These instructions are transmitted in particular through the tag management tool that they have integrated into their site and through the configuration of the tool. Indeed, the site manager can choose different parameters in order to set, for example, the data retention period. The Google Analytics feature also allows site managers to

monitor and maintain the stability of their site, for example by being informed of certain events such as a peak in traffic or, on the contrary, the fact that there is no traffic at all. Google Analytics also allows site managers to assess and optimize the effectiveness of advertising campaigns conducted using other Google tools.

In this context, Google Analytics collects, among other things, the user's http request, information on his browser and on his operating system. […] an http request, for any page, contained details of the browser and the terminal making the request, such as the domain name and information relating to the browser such as its type, its referrer (“ *referer* ”) and his language. Google Analytics places and reads cookies on the user's browser to help evaluate the user's session and other page request information.

When this information is collected, it is transmitted to the Google Analytics servers. […] all of the data collected through Google Analytics was hosted in the United States.

Thus, data collected on the website […] via Google Analytics is transferred to the United States.

Regarding these transfers, it appears from the documents in the file that the contract that binds […] concerning the Google Analytics functionality refers to an appendix entitled “ *Google Ads Data Processing Terms* ”. This appendix contains standard contractual clauses intended to govern the transfer to the United States of America of personal data as part of the Google Analytics functionality. The company indicated that it did not have in its possession any elements leading to the conclusion that these clauses had not been respected.

[…] additional legal, organizational and technical measures to regulate data transfers within the framework of the Google Analytics functionality are implemented work.

It emerges from all of these elements that the company managing the website […], by deciding to implement the Google Analytics functionality on this site for evaluation and optimization purposes, has determined the means and purposes of the collection and processing of data collected as part of the integration of Google Analytics on its website and must be considered as data controller within the meaning of Article 4.7 of the GDPR.

III. On the qualification of personal data

It should be established that the data collected as part of the Google Analytics functionality and transferred to the United States of America constitutes personal data.

Article 4.1 of the GDPR defines personal data as “ *any information relating to an identified or identifiable natural person (hereinafter referred to as “data subject”); an "identifiable natural person" is deemed to be a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more specific elements specific to his physical, physiological, genetic, psychic, economic, cultural or social identity* ”.

It should be noted that online identifiers, such as IP addresses or information stored in cookies can be used as a means to identify a user, especially when combined with other similar types of information. This is illustrated by recital 30 of the GDPR which provides that an online identifier associated with a natural person, such as an IP address or a cookie, can " *leave traces which, in particular when combined with identifiers unique and other information received by the servers, can be used to create profiles of natural persons and to identify these persons* ".

In the event that the data controller claims not to have the ability to identify the user through the use of this type of identifiers (alone or combined with other data), he should demonstrate the means implemented to ensure the anonymity of the identifiers collected. In the absence of such a demonstration, these identifiers cannot be qualified as anonymous.

Therefore, it should be examined to what extent the implementation of Google Analytics on a website allows the operator of the website […] to make a data subject (a visitor to the website in question) identifiable.

In its response, […] argues that the following categories of personal data are processed as part of the Google Analytics functionality: - a visitor ID (ID of the Google Analytics visitor cookie, i.e. the Google Analytics " *customer ID* "); - for visitors who have authenticated to the website through a user account, a internal identifier […]; - the order identifiers, if applicable; - IP addresses.

The company claims that IP addresses are " *anonymized* ", without specifying what process is applied to anonymize these addresses. However, the company qualifies this data as personal data.

With regard to visitor identifiers, it should be noted that these are unique identifiers, the purpose of which is to differentiate individuals. In this case, these identifiers may also be combined with other information, such as the address of the site visited, metadata relating to the browser and the operating system, the time and data relating to the visit of the website and IP address. This combination makes it possible to reinforce their discriminating character.

This is why, several elements when they are cross-checked, can make it possible to individualize the visitors of the website […], on which Google Analytics is implemented. It is not necessary to know the visitor's name or postal address since, in accordance with recital 26 of the GDPR, such individualization of persons may be sufficient to make them identifiable.

If it were to be decided otherwise, the scope of the right to data protection, guaranteed by Article 8 of the Charter of Fundamental Rights, would be reduced. In effect, it would allow companies to individualize individuals and associate personal information with them (such as their visit to a specific website) without granting individuals protection against such individualization. Such an assessment, which would reduce the level of protection of

individuals, would also be contrary to the case law of the Court of Justice of the European Union which has repeatedly held that the scope of the GDPR has a very broad definition (see, for example, Cÿ439/19, point 61) .

The CNIL also notes that for users of the website […] who have identified themselves through a user account, or those who have placed an order, the data is directly linked to identifying data.

In addition, […] as part of the use of Google Analytics, and under certain conditions of setting up the Google account, Google is informed that a user connected to his Google account has visited a particular site. Personal data relating to this account is therefore collected.

Therefore, it must be considered that the data in question must be considered as personal data within the meaning of Article 4 of the GDPR.

IV. On the breach of the obligation to regulate the transfer of personal data staff outside the European Union

Article 44 of the GDPR provides: " *A transfer, to a third country or to an international organisation, of personal data which are or are intended to be the subject of processing after this transfer may only take place if , subject to the other provisions of this Regulation, the conditions set out in this chapter are complied with by the controller and the processor, including for onward transfers of personal data from the third country or international organization to another third country or to another international organisation. All the provisions of this chapter are applied in such a way that the level of protection of natural persons guaranteed by this regulation is not compromised.* »

Chapter V of the Regulation provides for various instruments to ensure a level of protection substantially equivalent to that guaranteed within the European Union, pursuant to Article 44 of this text: adequacy decisions (Article 45);

- appropriate safeguards (Article 46);

In the absence of an equivalent level of protection, it establishes derogations for situations particular (section 49).

In the present case, it must be examined whether the data transfers in question to the United States of America comply with Article 44 of the Regulation and, in particular, whether these transfers are based on one of the aforementioned instruments and whether appropriate measures have been adopted.

4.1 Suitability decisions

In the judgment of July 16, 2020 (C-311/18), the Court of Justice of the European Union invalidated Commission Implementing Decision (EU) 2016/1250 of July 12, 2016, in accordance with the Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the European Union-United States Privacy Shield, without maintain its effects.

In the absence of another relevant adequacy decision, the transfers at issue cannot be based on Article 45 of the GDPR.

4.2 Appropriate safeguards

Article 46.1 of the Regulation provides " *In the absence of a decision pursuant to Article 45(3), the controller or processor may not transfer personal data to a third country or to an organization international community only if it has provided appropriate safeguards and provided that the persons concerned have enforceable rights and effective legal remedies.* »

Article 46.2 of the Regulation provides that the " *appropriate safeguards referred to in paragraph 1 may be provided, without this requiring specific authorization from a supervisory authority, by: […] (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);* ".

4.2.1 Standard data protection clauses

In this case, the company and Google have entered into standard contractual clauses for the transfer of personal data to the United States ("Google AdsData Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors"). These clauses are in line with those published by the European Commission in its decision 2010/87/EU.

In this context, it should be emphasized that the standard contractual clauses are an instrument of transfer within the meaning of Chapter V of the Regulation and have not been called into question as such by the Court of Justice in its judgment of July 16, 2020 (C-311/18). However, the Court considered that it followed from the contractual nature of these clauses that they could not bind the authorities of third countries. In particular, the Court considered that: " *If there are therefore situations in which, depending on the state of the law and the practices in force in the third country concerned, the recipient of such a transfer is able to guarantee the necessary data protection on the basis of the standard data protection clauses alone, there are others in which the stipulations contained in these clauses may not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. This is the case, in particular, when the law of that third country allows its public authorities to interfere with the rights of data subjects relating to that data.* »
(Cÿ311/18, paragraph 126).

However, it is not necessary to analyze in more detail the legal framework applicable to the United States of America insofar as the Court has already carried out such an analysis in the aforementioned judgment. The Court found, first, that the monitoring programs in question did not correspond to the minimum requirements attached, in EU law, to the principle of proportionality, so that it was not permitted to consider that monitoring programs based on these provisions are limited to what is strictly necessary (point 184). On the other hand, the Court found that the legal framework in question did not confer on the persons concerned rights enforceable against the American authorities before the courts, so that these persons did not have a right to an effective remedy (point 192) .

The analysis of the Court of Justice is relevant in this case insofar as Google LLC (as a data importer in the United States) must be qualified as a provider of

electronic communications within the meaning of Section 50 US. Code § 1881(b)(4) and is, therefore, subject to surveillance by US intelligence agencies pursuant to Section 50 US. Code § 1881a ("FISA 702"). Google LLC is therefore under an obligation to provide the US government with personal data that would be required under FISA 702.

It appears from Google's transparency report that Google LLC is regularly the recipient of such access requests by the intelligence services of the United States of America.

Thus, on the one hand, the Court of Justice declared invalid the decision of adequacy with the United States of America, because of the possibilities of access of the American intelligence services. On the other hand, the standard contractual clauses cannot, on their own, ensure a sufficient level of protection as required by Article 44 of the GDPR insofar as the guarantees they provide are left unapplied in the event of access by said intelligence services. The Court of Justice drew the following conclusion: " *It thus appears that the standard data protection clauses adopted by the Commission under Article 46(2)(c) of the same regulation are intended solely to provide controllers or their processors established in the Union contractual guarantees applying uniformly in all third countries and, therefore, independently of the level of protection guaranteed in each of them. Insofar as these standard data protection clauses cannot, having regard to their nature, provide guarantees which go beyond a contractual obligation to ensure that the level of protection required by Union law is complied with, they may require, depending on the situation prevailing in a particular third country, the adoption of additional measures by the controller in order to ensure compliance with this level of protection.* (item 133).

4.2.2 Adoption of additional safeguards

In his Recommendations 01/2020 of 18 June 2021, the EDPS clarified that where the assessment of the law or practice of the third country reveals that there are elements likely to undermine the effectiveness of the appropriate safeguards offered the instrument of transfer referred to in Article 46 of the GDPR which the exporter uses in the context of a particular transfer – which is the case here, following the assessment carried out by the CJEU – the exporter must suspend the transfer or put in place additional measures. The EDPS notes in this regard that " (a)ny *additional measure can only be deemed effective within the meaning of the judgment of the CJEU in the Schrems II case if and insofar as it remedies – taken alone or in combination with others – to shortcomings identified in the assessment of the legal situation and applicable practices of the third country that the exporter has carried out.* (item 75).

The measures to complete the standard data protection clauses can be classified into three categories: contractual, organizational and technical (see, for this purpose, point 47 of recommendations 01/2020).

With regard to contractual measures, the EDPS noted that such measures: " […] *can complement and reinforce the safeguards that the instrument of transfer and the relevant legislation of the third country […] may offer. Given the contractual nature of the measures, which are generally not likely to bind the authorities of the third country when they are not parties to the contract, these measures should be combined with other measures technical and organizational to provide the required level of data protection. […]* " (paragraph 99).

As regards the organizational measures, the EDPS considered that the " […] *selection and implementation of one or more of these measures does not necessarily and systematically guarantee that the transfer will meet the standard of essential equivalence established by Union law. Depending on the particular circumstances of the transfer and the assessment of the legislation of the third country, organizational measures are necessary to supplement the contractual and/or technical measures in order to guarantee a level of protection of personal data essentially equivalent to that guaranteed within the EEA* " (paragraph 128).

With regard to technical measures, the EDPS underlined that these " [...] *measures will be particularly necessary in the event that the law of that country imposes on the data importer obligations which are contrary to the safeguards offered by the transfer instruments referred to in Article 46 of the GDPR and which are, in particular, likely to affect the contractual guarantee of an essentially equivalent level of protection against access by the public authorities of this country to this data* " (point 77). It adds that " *The measures listed [in the guidelines] aim to ensure that access by public authorities of third countries to the data transferred does not undermine the effectiveness of the appropriate safeguards contained in the transfer instruments referred to in article 46 of the GDPR. These measures are necessary to guarantee a level of protection essentially equivalent to that guaranteed within the EEA, even if the access of public authorities is in accordance with the legislation of the country of the importer, when this access goes beyond what is necessary and proportionate in a democratic society. These measures aim to prevent any potentially illicit access, by preventing the authorities from identifying the data subjects, inferring information about them, distinguishing them in another context or associating the transferred data with other data sets which could contain, in particular, online identifiers provided by devices, applications, tools and protocols used by data subjects in other contexts* " (point 79).

4.2.3 Additional measures implemented by Google

Google LLC, as the recipient of the data, has adopted contractual, organizational and technical measures to supplement the standard data protection clauses. […]

As prescribed by the CJEU and the EDPS, it is necessary to verify whether the additional measures adopted by Google LLC are effective, that is to say that they respond to the particular problem of the possibility of access to the services of US intelligence to the data at issue.

With regard to the " *legal and organizational measures* " adopted, it should be noted that neither the notification of users (if this is possible), nor the publication of a transparency report or a request management policy government access requests (" *policy on handling government requests* ") does not specifically prevent or reduce access by US intelligence services. Further, it is not clear from the evidence to what extent Google LLC's careful review of the lawfulness of each request is an effective additional measure. Indeed, according to the CJEU, even lawful requests from US intelligence services do not comply with the requirements of European data protection law.

With regard to the " *technical measures* " adopted, it should be noted that it has not been clarified, neither by Google LLC nor by the company how the measures described - such as the protection of communications between Google services , the protection of data in transit between data centers, the protection of communications between users and websites or on-site security – help prevent or reduce the possibilities of access by American intelligence services on the basis of the American legal framework.

With regard to encryption techniques, such as those for data stored in data centers, mentioned in particular by Google LLC as a technical measure, it should be noted that Google LLC, as data importer has in all the cases the obligation to grant access or to provide the imported data which is in its possession, including the encryption keys necessary to make the data intelligible (see recommendations 01/2020, point 81). In other words, as long as Google LLC has the ability to access natural persons' data in clear text, such technical measures cannot be considered effective in this case.

With regard to Google LLC's argument that Google Analytics data that is transferred by site managers is pseudonymized, it should be noted that universally unique identifiers (UUIDs) do not correspond to the definition of the article 4.5 GDPR. Indeed, while pseudonymization can be a technique that contributes to the protection of privacy, unique identifiers – as previously emphasized – have the specific purpose of individualizing users, and not of serving as a guarantee. In addition, it has also been pointed out above how the combination of unique identifiers with other elements (such as browser or device metadata or IP address) and the possibility of linking such information to an account Google or an account […] allow
in any case to be able to identify an individual.

With regard to the " *optional technical measure* " put forward by Google LLC, which consists of an IP address anonymization function, it should be noted first of all that such a measure is optional and is not not applicable to all transfers. Furthermore, it does not appear not from Google's response if this anonymization takes place before the transfer or if the entire IP address is in any case transmitted to the USA and only shortened in a second step after the transfer to the USA United. Thus, from a technical point of view, there is a potential access to the entire IP address before it is shortened.

Consequently, the additional measures adopted, as presented by Google, are not effective insofar as none of them solves the specific problems of the present case. Indeed, none of them prevent the American intelligence services from accessing the data in question or render this access ineffective.

4.3. Exceptions provided for in Chapter V of the Regulations

Article 49 of the Regulations provides “ *1. In the absence of an adequacy decision under Article 45(3) or appropriate safeguards under Article 46, including binding corporate rules , a transfer or set of transfers of personal data to a third country or to an international organization may only take place under one of the following conditions:*

(a) the data subject has given explicit consent to the intended transfer, after having been informed of the risks that this transfer could entail for her due to the absence of decision of adequacy and appropriate safeguards;

b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the request of the data subject; […] "

The company argues that the transfer could be based on Article 49.1.a of the GDPR stating that the data subject can refuse that Google can track his visit to the website.

However, the consent by a user to the deposit of tracers during his visit to the website cannot be considered as equivalent to " *explicit consent to the proposed transfer, after having been informed of the risks that this transfer could entail for him due to the 'absence of adequacy decision and appropriate safeguards* ' within the meaning of Article 49.1.a of the Regulation. In this regard, it may be noted that the company, far from establishing that such consent has been obtained, does not put forward any information relating to these elements which would be transmitted to visitors to the website.

The company also invokes Article 49.1.b of the Regulations insofar as these functionalities are necessary for the proper functioning of the website and for the detection of anomalies.

This argument is nevertheless not supported by any precise element and, above all, the company does not establish that there is a contractual relationship between it and all the users of its website.

Consequently, the company cannot rely on Article 49 of the Regulations to justify the transfers in question.

4.4. Conclusion

Consequently, it must be concluded that the company cannot rely on any of the instruments provided for in Chapter V of the Regulation to justify the transfer of personal data of visitors to its website, and in particular unique identifiers, addresses IP, browser data and metadata, to Google LLC in the United States.

Thus, due to this transfer of data, the company compromises the level of protection of the personal data of the persons concerned, as guaranteed by Article 44 of the GDPR.

Consequently, […] **is given formal notice within one (1) month of notification of this decision and subject to the measures that it could have already adopted, of:**

- **bring the processing relating to the Google Analytics functionality into compliance with articles 44 and following of Regulation (EU) 2016/679 of the Parliament European Parliament and of the Council of 27 April 2016, if necessary, ceasing to deal with personal data under the current version of Google Analytics;**

- **justify to the CNIL that the aforementioned request has been complied with, and this within the time limit.**

At the end of this period, if […] **has complied with this formal notice, it will be considered that this procedure is closed and a letter will be sent to him to this effect.**

Conversely, if […] **has not complied with this formal notice, it is recalled that a rapporteur may be appointed to request that the Restricted Committee impose one of the sanctions provided for in Article 20 of the amended law of January 6, 1978.**

The president

Marie-Laure DENIS