Draft decision No. [redacted] ordering the company [redacted] to comply

(No. [redacted]

The Chair of the Commission Nationale de l'Informatique et des Libertés (CNIL),

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

Having regard to the French Data Protection Act No. 78-17 of 6 January 1978, as amended, particularly Article 20;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL (French Data Protection Agency);

Having regard to Decision No. 2020-257C of 12 October 2020 of the Chair of the CNIL instructing the General Secretary to carry out, or have carried out, an audit of the data processing activities accessible from the domain [redacted] or concerning personal data collected from this domain;

Having regard to referral No.[redacted]

Having regard to the other exhibits;

I. <u>The procedure</u>

[redacted] (hereinafter "the company" or [redacted]), whose registered office is located at [redacted], is a retailer of sport articles in specialized stores.

On 19 August 2020, the Commission nationale de l'informatique et des libertés (French data protection authority, hereinafter "CNIL") received a complaint (no. 20013890) relating to the transfer of personal data of the complainant (represented by the association [redacted]), to the United States of America, collected during his visit to the website [redacted]. [redacted] has filed 101 complaints in the 27 Member States of the European Union and the three other members of the European Economic Area (EEA) against 101 data controllers alleged to transfer personal data to the United States.

Pursuant to decision No. 2020-257C of the CNIL Chair dated [redacted], a CNIL delegation carried out a documentary audit by sending a questionnaire to [redacted] on [redacted] and a request for further information on [redacted]. The company replied in letters [redacted]. The questionnaires concerned the

transfer of data of visitors to the French language version of the website [redacted], which uses the Google Analytics service.

[redacted] the company informed the CNIL that it had decided to integrate the Google Analytics functionality on its website [redacted] and that the statistics obtained via Google Analytics concerned individuals in several member states of the European Union. The processing activity resulting from the integration of the Google Analytics functionality on its website therefore appears to meet the definition of cross-border processing within the meaning of Article 4.23.b) of the GDPR.

[redacted].

Pursuant to Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "GDPR" or the "Regulation"), [redacted], the CNIL informed all European supervisory authorities of its competence to act as lead authority regarding the cross-border processing implemented by the company, this competence deriving from the fact that the company's principal place of business is located in France.

Within the meaning of Article 4, point 22 of the GDPR, [redacted] data protection authorities are concerned, namely the authorities of [redacted]

On 28 January 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 draft decision did not give rise to any relevant and reasoned objections.

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

The responses [redacted] sent to the audit delegation revealed that the company integrated the Google Analytics feature on the website [redacted]. This feature has been implemented for the purpose of measuring its audience (volume of traffic, number of unique visitors, origin of connection, type of terminal used, conversion rate of visitors into buyers, etc.); of analysing the path of visits in order to correct or improve the site; of understanding and having visibility on the display and ordering of products as well as their attractiveness; and finally of measuring and anticipating connection peaks.

[redacted]

[redacted]

Google Analytics works by including a piece of JavaScript code on the pages of a website. When a user visits a webpage, this code triggers the uploading of a JavaScript file and then performs the tracking operation for Google Analytics. The tracking operation consists of recovering data relating to the query through various means and sending this information to the Google Analytics servers.

Website managers who integrate the Google Analytics service may send instructions to Google for the processing of data collected through Google Analytics. These instructions are transmitted through the tag manager that manages the tracking code they have integrated into their website and through the tag manager settings. The website manager can apply different settings, for example, regarding the data retention period. The Google Analytics feature also allows website managers to monitor and maintain the stability of their website, for example by keeping them informed of certain events such as a peak in audience or the fact that there is no traffic at all. Google Analytics also allows website managers to measure and optimise the effectiveness of advertising campaigns conducted using other Google tools.

In this context, Google Analytics collects among other things the user's http query and information about the user's browser and operating system, among other things. [redacted] an http request, for any page, contains details of the browser and the device making the query, such as the domain name and browser information such as its type, referer, and language. Google Analytics stores and reads cookies on the user's browser to evaluate the user's session and other information on the query.

When this information is collected, it is transmitted to the Google Analytics servers. [redacted] indicated that all data collected through Google Analytics are hosted in the United States.

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

As regards these transfers, it appears from the exhibits that the contract [redacted] concerning the Google Analytics feature refers to an appendix entitled Google Ads Data Processing Terms. This appendix contains standard contractual clauses governing the transfer of personal data to the United States of America under the Google Analytics service. The company indicated that it does not have any information that would enable to assess with certainty whether these clauses are respected.

[redacted] it has implemented additional legal, organisational and technical measures to regulate data transfers under the Google Analytics service.

All of these elements show that, by deciding to implement the Google Analytics feature on this website for evaluation and optimisation purposes, the company managing the website [redacted] determined the means and purposes of the collection and processing of the data obtained further to the integration of Google Analytics on its website and should be considered the data controller within the meaning of Article 4.7 of the GDPR.

III. <u>On the qualification of personal data</u>

It can be established that the data collected under the Google Analytics feature and transferred to the United States of America constitute personal data.

Article 4.1 of the GDPR defines personal data as *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 factors specific to*

the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

It should be noted that online identifiers, such as IP addresses or information stored in cookies can commonly be used to identify a user, particularly when combined with other similar types of information. This is illustrated by Recital 30 GDPR, according to which the assignment of online identifiers such as IP addresses and cookie identifiers to natural persons or their devices may "*leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them*." In the particular case where the controller would claim to not have the ability to identify the user through the use (alone or combined with other data points) of such identifiers, he would be expected to disclose the specific means deployed to ensure the anonymity of the collected identifiers. Without such details, they cannot be considered anonymous.

Therefore, it is necessary to examine to what extent the implementation of Google Analytics on a website allows the website manager and [redacted] to render a data subject (a visitor of the website in question) identifiable.

The responses [redacted] revealed that the following categories of data are processed under the Google Analytics feature:

- data relating to orders placed, which are not directly identifying;
- an identifier of the visitor cookie Google Analytics;
- the visitor's IP address.

The company explains that it changes the identifiers of the Google Analytics cookies by randomly determining a new identifier. It also specifies that the last bytes of IP addresses are removed.

With regard to visitor identifiers, it should be noted that these are unique identifiers intended to differentiate individuals and thus identify them by allowing the players in question to be able to "recognize" them later. The fact that the identifiers are modified by the data controller to be replaced by a new random identifier does not remove their uniqueness, which makes it possible to follow an individual when browsing a site that integrates the Google Analytics feature.

In the present case, these identifiers may also be combined with other information, such as the address of the website visited, metadata relating to the browser and operating system and the time and data relating to the visit to the website. Moreover, the communication of an IP address, even if truncated, can contribute to the subsequent re-identification of the individual concerned. This combination of information enables to reinforce their discriminatory nature insofar as [redacted] has all this information associated with the unique identifier.

For this reason, when several elements are combined, they can make it possible to individually identify visitors to the [redacted] website, on which Google Analytics is implemented. It is not required to know the actual visitor's name or (physical) address since, in accordance with recital 26 of the GDPR, such singling out of individuals is sufficient to make the visitor identifiable.

Should it be decided otherwise, the scope of the right to data protection, guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, would be undermined as it

would allow companies to specifically single out individuals along with personal information (such as when they visit a specific website) while denying them any right of protection against such singling out. Such a restrictive view that would undermine the level of protection of individuals is also not line with the case law of the Court of Justice of the European Union, which repeatedly ruled that the scope of the GDPR has to be understood in a very wide manner (see, for example, C-439/19, paragraph 61).

Moreover, i[redacted], in the context of using Google Analytics, and under some Google account settings, Google is informed that a user connected to a Google account has visited a particular website. Personal data related to this account is then collected, including the name of its user, and linked to the unique identifier assigned as part of the Google Analytics feature. All data related to this user can therefore be attributed to an identified individual.

As a result, it must be considered that the data in question should be regarded as personal data within the meaning of Article 4 of the GDPR.

IV. On the breach of the obligation to transfer users' data to non-adequate countries in accordance with the appropriate safeguards

Article 44 of the GDPR states: "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*"

Chapter V of the Regulation provides for various tools to ensure a level of protection substantially equivalent to that guaranteed within the European Union, pursuant to Article 44 of the Regulation:

- adequacy decisions (Article 45);
- appropriate safeguards (Article 46);

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

In the present case, it must be verified whether the export of personal data to the United States of America comply with Article 44 GDPR and, in particular, whether the export was based on one of these grounds, and if it was, if the relevant measures were taken.

4.1 Adequacy decisions

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

In the absence of another relevant adequacy decision, the transfers in question may not be based on Article 45 of the GDPR.

4.2 Appropriate safeguards

Article 46.1 of the Regulation provides that "*In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.*"

Article 46.2 of the Regulation provides that "*The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation 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 the present case, the company and Google have entered into standard contractual clauses for the transfer of personal data to the United States (Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors). These clauses are in line with those published by the European Commission in Decision 2010/87/EU.

In this context, it must be emphasised that standard contractual clauses are a transfer tool within the meaning of Chapter V of the Regulation and were not challenged as such by the Court of Justice in its judgement of 16 July 2020 (C-311/18). However, the Court considered that it stemmed from the contractual nature of these clauses that they could not be binding on the authorities of third countries. In particular, the Court held that: "*Therefore, although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses, there are others in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates*" (C-311/18, point 126, emphasis added).

A further analysis of the legal situation of the USA is not required though, as the CJEU has already provided such analysis in its aforementioned judgement. Indeed, the Court found that the surveillance programmes in question do not correlate to the minimum safeguards arising from the principle of proportionality under Union law, such that the surveillance programmes based on these provisions cannot be regarded as limited to what is strictly necessary (point 184). Moreover, the Court found that the legal framework in question did not confer on data subjects rights actionable in the courts against the US authorities, from which it follows that these persons have no right to an effective remedy (point 192).

The analysis of the CJEU is relevant in the present case, since Google LLC (as importer of the data to the USA) is to be qualified as a provider of electronic communications services within the meaning of 50 US. Code § 1881(b)(4) and is therefore subject to surveillance by US.

intelligence services in accordance with 50 US. Code § 1881a ("FISA 702"). Google LLC therefore has the obligation to provide the US government with personal data when requested FISA 702.

As can be seen in the Google Transparency Report, Google LLC is regular subject to such access requests by US. intelligence services.

The Court of Justice declared, on one hand, the adequacy decision with the United States of America invalid due to the access possibilities of US intelligence services, and, on the other hand, that the conclusion of SCCs cannot by themselves ensure a level of protection as required by Article 44 GDPR as the guarantees they provide are left unapplied when such access requests are taking place. Indeed, the CJEU concluded the following: "*It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection"* (point 133).

4.2.2 Implementation of additional safeguards

In its recommendations 01/2020 of 18 June 2021, the European Data Protection Board (EDPB) has clarified that where the assessment of the law and/or practices in force of the third country may impinge on the effectiveness of the appropriate safeguards of the transfer tools the exporter is relying on, in the context of his specific transfer, which is the case here following the assessment by the CJEU, the exporter has to either suspend the transfer or implement adequate supplementary measures. The EDPB notes in this respect that "*Any supplementary measure may only be deemed effective in the meaning of the CJEU judgement "Schrems II" if and to the extent that it – by itself or in combination with others - addresses the specific deficiencies identified in the assessment of the situation in the third country as regards its laws and practices applicable to the transfer*" (point 75).

Measures to supplement standard data protection clauses can be classified into three categories: contractual, organisational and technical (see point 47 of Recommendations 01/2020).

With regard to <u>contractual</u> measures, the EDPB noted that such measures: "*[…] may complement and reinforce the safeguards the transfer tool and relevant legislation of the third country may provide […]. Provided the nature of contractual measures, generally <u>not capable of binding the authorities of that third country</u> when they are not party to the contract, these measures may often need to be <u>combined with other technical and organisational measures</u> to provide the level of data protection required […]*" (point 99, emphasis added).

As regards <u>organisational</u> measures, the EDPB highlighted that "*[…] Selecting and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. Depending on the specific circumstances of the transfer and the <u>assessment performed on the legislation of the third country</u>, organisational measures are needed to <u>complement contractual and/or</u>*

technical measures, in order to ensure a level of protection of the personal data essentially equivalent to that guaranteed within the EEA" (point 128, emphasis added).

With regard to technical measures, the EDPB pointed out that "*[…] These measures will be especially needed where the law of that country imposes on the data importer obligations which are contrary to the safeguards of Article 46 GDPR transfer tools and are, in particular, capable of impinging on the contractual guarantee of an essentially equivalent level of protection against access by the public authorities of that third country to that data*" (point 77, emphasis added). It added that *"The measures listed [in the guidelines] are intended to ensure that access to the transferred data by public authorities in third countries does not impinge on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. These measures would be necessary to guarantee an essentially equivalent level of protection to that guaranteed in the EEA, even if the public authorities' access complies with the law of the importer's country, where, in practice, such access goes beyond what is necessary and proportionate in a democratic society. These measures aim to preclude potentially infringing access by preventing the authorities from identifying the data subjects, inferring information about them, singling them out in another context, or associating the transferred data with other datasets that may contain, among other data, online identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts*" (point 79, emphasis added).

4.2.3 Supplementary measures implemented by Google

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

Taking the considerations of the CJEU and the EDPB into account, it must now be verified whether or not the supplementary measures adopted by Google LLC are effective, meaning they address the specific issue of access possibilities of US intelligence services.

With regard to the *legal and organisational measures* adopted, it must be noted that neither the notification of users – should such notification even be permissible – nor the publication of a Transparency Report or a publicly available „policy on handling government requests" in fact prevent or reduce access possibilities of US intelligence services. Furthermore, it remains unclear how Google LLC's „careful review of each request" on its permissibility is effective as supplementary measure, considering that according to the CJEU, permissible (legal) requests of US intelligence services are not in line with the requirements of the European Data Protection Law.

With regard to the *technical measures* adopted, it should be noted that it has not been clarified, either by Google LLC or by the company, how the measures described – such as the protection of communications between Google's services, the protection of data in transit between data centres, the protection of communications between users and websites, or "on-site security" – in fact prevent or reduce the possibilities of access by US intelligence services on the basis of the US legal framework.

As far as encryption technologies are concerned – such as for „data at rest" in data centres, as specifically mentioned by Google LLC as technical measure – it has to be noted that Google LLC as data importer nonetheless has an obligation to grant access or to turn over imported

personal data in their possession, including any cryptographic keys necessary to render the data intelligible (see Recommendations 01/2020, point 81). In other words: As long as Google LLC has the possibility to access the data of natural persons in clear text, such technical measure cannot be deemed effective in the present case.

As far as Google LLC brings forward that „(t)o the extent Google Analytics Data for measurement transferred by website owners is personal data, it would have to be regarded as pseudonymous", it must be noted that universal unique identifiers (UUIDs) do not fall under the definition of Article 4.5 of the GDPR. While pseudonymisation may be a privacy-enhancing technique, the unique identifiers have, as already outlined above, the specific intention to single out users, not to act as safeguard. Apart from this, it has also been outlined above why the combination of unique identifiers with other elements (such as browser or device meta data) and the possibility to link such information to a Google Account in any case make an individual identifiable.

Therefore, the supplementary measures adopted, as presented by Google, are not effective insofar as none of them addresses the specific issues in the present case, meaning none of them prevent access possibilities of US intelligence services or render these accesses ineffective.

4.3. The derogations provided for in Chapter V of the Regulation

The company asserted that, the transfer of the data at issue outside the European Union is not currently based on any other tool provided for by Article 49 of the GDPR.

4.4. Conclusion

Therefore, it must be concluded that the company cannot invoke any of the tools 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, IP addresses, browser data and metadata, to Google LLC in the United States.

Accordingly, with this transfer of data, the company undermines the level of personal data protection of data subjects as guaranteed in Article 44 of the GDPR.

Consequently, [redacted], located at [redacted], is hereby ordered to do the following, within one (1) month of notification of this decision, that might be renewed once, and subject to any measures it may have already implemented:

- **bring the data processing activity under the Google Analytics service into compliance with Articles 44 et seq. of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, notably by ceasing processing activities which relate to the current version of the tool Google Analyctics;**

- **provide supporting documentation to the CNIL confirming that the aforementioned request has been complied with within the time limit.**

At the end of that period, if [redacted] has complied with this order, it will be considered that these proceedings are closed and a letter will be sent to it to that effect.

Conversely, if [redacted] has not complied with this order by the end of that period, a rapporteur will be appointed to request the restricted committee to issue one of the penalties provided for by Article 20 of the French Data Protection Act of 6 January 1978, as amended.

The Chair

[redacted]