Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision in case with national reference number, DI-2020-11397. Only the Swedish version of the decision is deemed authentic

Registration number:
DI-2020-11397

Date of decision:
2023-06-30

Final decision under the General Data Protection Regulation– CDON AB transfers of personal data to third countries

Table of contents

Mailing address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection finds that the investigation has shown that CDON AB processed personal data in breach of Article 44 of the GDPR1 by using the Google Analytics tool provided by Google LLC on its website www.cdon.fi, and thus transferring personal data to third countries without fulfilling the conditions laid down in Chapter V of the Regulation, since 14 August 2020 and until the date of this Decision.

Pursuant to Article 58(2)(d) of the GDPR, CDON AB is required to ensure that the company's processing of personal data in the context of the company's use of the Google Analytics tool complies with Article 44 and the other provisions of Chapter V of the GDPR. In particular, CDON AB shall cease to use the version of the Google Analytics tool used on 14 August 2020, unless sufficient safeguards have been taken. The measures shall be implemented no later than one month after the date of entry into force of this Decision.

On the basis of Articles 58(2) and 83 of the GDPR, IMY decides that CDON AB shall pay an administrative fine of SEK 300 000 (three hundred thousand) for infringement of Article 44 of the GDPR.

1. Report on the supervisory case

1.1 Processing

The Swedish Integrity Authority for Protection Authority (IMY) has initiated supervision regarding CDON AB (hereinafter CDON or the company) due to a complaint. The complaint has claimed a breach of the provisions of Chapter V of the GDPR related to the transfer of the complainant's personal data to third countries. The transfer is alleged to have taken place when the complainant visited the company's website, www.cdon.fi (hereinafter "the company's website" or the "Website") through the Google Analytics tool (hereinafter the Tool) provided by Google LLC.

The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Austria) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned are the data protection authorities in Germany, Norway, Estonia, Denmark, Portugal, Spain, Finland and Austria.

---

[1] 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 he processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.2 What is stated in the complaint

The complaint has essentially stated the following.

On 14 August 2020 the complainant visited the CDON website. The complainant visited the controller's website, while being logged in to the Google/ Facebook account associated with the complainant's email address. On the website, the controller has embedded a JavaScript code for Google/ Facebook services including "Google Analytics" or "Facebook Connect". In accordance with paragraph 5.1.1(b) of the terms and conditions of Google's processing of personal data for Google's advertising products and also Google's terms and conditions for processing the New Google Ads Processing Terms, for Google Advertising Products, Google processes personal data on behalf of the controller (i.e. CDON) and is therefore to be classified as the company's data processor.

During the visit of the company's website, CDON processed the complainant´s personal data, at least the complainant's IP address and the data collected through cookies. Some of the data has been transferred to Google. In accordance with Section 10 of the Terms and Conditions on the Processing of Personal Data for Google's Advertising Products, CDON has authorised Google to process personal data of the Applicant in the United States. Such transfer of data requires legal support in accordance with Chapter V of the GDPR.

According to the judgment of the Court of Justice of the European Union (CJEU), in Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II) [2], the company could no longer rely on an adequacy decision under Article 45 of the GDPR for the transfer of data to the United States. CDON should not base the transfer of data on standard data protection clauses under Article 46(2)(c) GDPR if the recipient of the personal data in the third country does not ensure appropriate protection with regard to Union law for the personal data transferred.

Google shall be classified as an electronic communications service provider within the meaning of 50 US Code § 1881 (4)(b) and is thus subject to surveillance by U.S. intelligence services in accordance with 50 US § 1881a (Section 702 of the Foreign Intelligence Surveillance Act, below "702 FISA").[3] Google provides the U.S. government with personal data in accordance with these provisions. CDON cannot therefore ensure adequate protection of the complainant's personal data when it is transmitted to Google.

1.3 What CDON has stated

CDON AB have in opinions on the 15 January 2021, 15 February 2022 and 31 August 2022, essentially stated the following.

1.3.1 Who has implemented the Tool and for what purpose etc.

The code for the Tool was embedded on the Website at the time of the complaint and is still embedded on the Website. The decision to embed the Tool on the Website was made by CDON, a company registered in Sweden. Data is collected from all persons

[2] Judgment of the Court of Justice of the European Union Facebook Ireland and Schrems (Schrems II), C-311/18, EU:C:2020:559.
[3] See https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881.htm and https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881a.htm.

visiting the Website, which is likely to include data subjects from more than one EU/EEA Member State.

CDON uses the Tool to get to know the traffic and uses the Website to make various business-critical decisions. It is possible to find out which product categories are most popular and how customers navigate, partly to find CDON and to end a purchase.

1.3.2 Recipients of the data
In the context of CDON's use of the Tool on the Website, personal data is only disclosed to Google.

1.3.3 The data processed in the Tool and what constitutes personal data
The data processed in the context of CDON's use of the Tool are different characteristics or actions taken by the visitor on the Website, such as:

1. What elements the user has seen while navigating and looking around the Site,
2. Clicked on an Image/Banner on the Website,
3. Added or removed something to the cart,
4. Came to checkout or completed a purchase,
5. Clicked on suggestions for accessories on product pages or added something to the wishlist,
6. If the user is a member of the CDON customer club; and
7. The search string used by the user to search internally on the Website.

In addition to this data, Google also has access to the IP address of the respective user.

1.3.4 Categories of persons concerned by the treatment
The categories of persons concerned by the processing are all categories of persons who visit the Website. CDON has no means of distinguishing if data on particularly vulnerable persons are processed. This is because CDON only processes anonymous "behavioural data" regarding how a user navigates the Website. The information processed by CDON is no more than the transfer of the information to Google. CDON cannot identify individual users before or after disclosure to Google. The category of persons a unique user belongs to is therefore unknown to CDON.

1.3.5 When the code for the Tool is executed and recipients are accessed
Immediately after the Website has finished loading into the user's browser, information about the location of the user on the Website has been transmitted to Google. Since 12 January 2021, CDON has activated a tool that requires the respective user's consent to integrate and run the content of the Tool into the user's browser.

1.3.6 How long the personal data are stored
Data and other information are not stored by CDON, but are transmitted by CDON to Google in real time. CDON's assessment is that the anonymisation of IP addresses described below means the data transferred to Google can no longer be linked to a specific individual and are therefore not personal data. Google will only store personal

data until the IP addresses are truncated[4]. According to Google, truncation is executed as soon as technically possible.

1.3.7 The countries in which personal data are processed
The data transmitted to the Tool is stored, for example in the United States.

1.3.8 CDON's relationship with Google LLC
CDON share the assessment made by Google regarding the allocation of personal data, whereby Google is deemed to process data in the context of CDON's use of the Tool as a data processor for CDON. CDON acts as data controller.

The terms that apply to the tool are both Google's Terms of Service and Google's data processing terms.

The sharing of personal data by Google and CDON is set out in the Google Ads Data Processing Terms.

1.3.9 Ensure that processing is not carried out for the purposes of the recipients
CDON has not had any reason to assume that Google does not meet the requirements of the Google Ads Data Processing Terms, so that its compliance with those terms has not yet been further verified by CDON.

1.3.10 Description of CDON's use of the Tool
CDON uses the Tool in order to get to know the traffic on the Website and to be able to make various business-critical decisions based on that information. For example, it is possible to find out which product categories are most popular and how customers navigate the Website to find CDON and to end a purchase.

1.3.11 Own checks on transfers affected by the judgment in Schrems II
Following the Schrems II judgment, CDON has taken measures in the form of identifying which of CDON's partners are located in countries outside the EU/EEA and, in relation to the respective partners, requested information on the additional security measures they have taken as a result of the ruling.

On October 26, 2020, CDON requested information from Google regarding the effect of CDON's embedding of the Code for the Tool on the Website. Google has not returned in response to CDON's request for information and, for this reason, in addition to repeating the request to Google and reminding of replies, CDON has sought publicly available information on the actions taken by Google as a result of the ruling.

According to publicly available information from Google, in addition to the Standard Contractual Clauses, Google has taken the following additional safeguards in relation to the Tool:

- Google ensures the secure transfer of JavaScript libraries and measurement data using the HTTP HSTS (Strict Transport Security) encryption protocol.
- The Tool has been certified according to the internationally accepted independent safety standards ISO 27001.

[4] Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255).

In addition to these actions, CDON has also chosen to activate IP anonymisation in the code of the tool, which means that IP addresses are truncated. IP anonymisation means that the last octet of IPv4 addresses and the last 80 bits of IPv6 addresses are deleted immediately after the addresses have been sent to the Tool Collection Network. Since CDON's view is that it is the IP addresses that cause the other data collected and transmitted using the Tool to be considered personal data, CDON's assessment is that the truncation of the IP addresses means that no information transmitted to Google is considered personal data after the IP anonymisation/trunking has been carried out.

1.3.12 Transfer tools under Chapter V of the GDPR
Transfers of personal data to recipients in third countries under CDON's use of the Tool are carried out on the basis of the European Commission's Standard Contractual Clauses (2010/87/EU).

In accordance with the versions of Google's data processing terms in force since 12 August 2020, Google and CDON have entered into EU Standard Contractual Clauses for the transfer of data from an EU controller to a data processor outside the EU, based on template 2010/87/EU of the European Commission.

1.3.13 Verification of obstacles to compliance in third country legislation
In order to ensure compliance with the contractual obligations set out in the standard contractual clauses, CDON has sent the request for information to Google regarding third country transfer described above and CDON has received no reply.

1.3.14 What information is covered by the definition of personal data
It is important to distinguish between the concepts of being able to distinguish users and not being able to identify a specific individual. The latter, identification of a specific individual is not the purpose of the use of the Tool, nor is it possible with the information collected by unique identifiers (which may be derived from the browser or device (i.e. CDON's Google Analytics account ID)) neither alone nor in combination with, inter alia, the information generated during visits to the Website (i.e. Web address (URL) and HTML title on that Website or browser information). CDON is of the firm opinion that IP addresses are necessary to process, among other things, the information generated when visiting the Website (i.e. URL (URL) and HTML title on that Website or information about browsers) may be considered personal data. CDON acknowledges that in certain circumstances dynamic IP addresses may be considered personal data. However, the differentiation of users made possible by the information collected by unique identifiers is not sufficient for a specific individual to be identified, with or without means such as, for example, disclosure, but only in combination with a full IP address that the information collected by unique identifiers and information generated by visits to the Website may constitute personal data.

The judgments Breyer[5] and M.I.C.M.[6] support the assessment that dynamic IP addresses are, in all cases, personal data. According to the Court of Justice, dynamic IP addresses may be regarded as personal data in relation to the provider of information or communication services concerned, not in relation to any operator accessing an IP address. In the judgement Breyer, concerning the assessment of the means which could reasonably be used to identify the person concerned, the Court held that, under German law, there were legal means enabling the provider of

[5] Judgment of the Court of Justice of the European Union Breyer, C-582/14, EU:C:2016:779.
[6] Judgment of the Court of Justice of the European Union M.I.C.M, C-597/19, EU:C:2021:492.

electronic information or communications services, in particular in the event of cyber attacks, to apply to the competent authority in order to take the necessary steps to obtain such information from the internet service provider and to initiate criminal proceedings. It may be questioned whether a U.S. authority with a truncated IP address, which may constitute one of 256 alternative IP addresses, has such lawful means as may reasonably be used to enable the identification of an individual, when, in the case of Breyer, a full IP address was even considered problematic in relation to the actual provider of that natural person's IT services.

1.3.15 Effectiveness of measure taken by Google and CDON
With reference to the answers above, in addition to the activation of IP anonymisation, CDON has not considered the implementation of accompanying measures as Google has informed that additional measures have been taken.

The truncation of IP addresses is an effective protection measure. Regardless of whether the IP addresses are truncated in connection with, or in connection with, the transmission of the information from CDON to Google. The truncation of the IP addresses means that the information stored on Google's servers in the United States does not constitute personal data. In a situation where the truncation takes place only after the data has been received by Google LCC, but at the latest immediately after receipt, the truncation means that all the data transmitted by CDON to Google and stored on Google's servers will not constitute personal data because the IP address, which is the unique identifier that causes the other information transmitted to constitute personal data, has been anonymised. The IP address without the last octet may be any of 256 alternative IP addresses and therefore *a* truncated IP address by thinning together with other information cannot be considered personal data.

1.3.16 Supplementary measures taken in addition to those taken by Google
During the handling of the case, CDON has thoroughly analysed and investigated the possibilities of switching to another solution that does not involve the use of the Tool. CDON have done preparations for such a change, which it will hopefully be able to implement promptly if IMY's final decision indicates that the Tool is not compliant with the GDPR and when that kind of decision becomes final. CDON's analysis shows that such a change (i.e. switch to a different solution) will be very burdensome for the company (in particular in comparison with other market players), so that it cannot be implemented before there is clarity in relation to what applies to the Tool as to what is a supplementary measure.

1.4 What Google LLC has stated

IMY has added to the case an opinion of Google LLC (Google) on 9 April 2021 submitted by Google to the data protection authority in Austria. The opinion answers questions asked by IMY and a number of regulators to Google in response to partial joint handling of similar complaints received by these authorities. CDON has been given the opportunity to comment on Google's opinion. Google's opinion shows the following about the Tool.

A JavaScript code is included on a web page. When a user visits (calls) a web page, the code triggers a download of a JavaScript file. After that, the Tool tracking operation, which consists of collecting information related to the call in different ways and sending the information to the server of the Tool, is performed.

A website manager who integrated the Tool on his website may send instructions to Google for the processing of the data collected. These instructions are transmitted via the so-called tag manager who manages the tracking code that the webmaster has integrated into his website and through the tag manager's settings. The person who integrated the tool can make different settings, for example regarding storage time. The Tool also enables those who integrated it to monitor and maintain the stability of their website, for example by keeping themselves informed of events such as peaks in visitor traffic or lack of traffic. The Tool also enables a website manager to measure and optimise the effectiveness of advertising campaigns carried out using other Google tools.

In this context, the Tool collects visitor's http calls and information about, among other things, the visitor's browser and operating system. According to Google, a http call for any page contains information about the browser and device making the call, such as domain names, and information about the browser, such as type, reference and language. The Tool stores and reads cookies in the visitor's browser to evaluate the visitor's session and other information about the call. Through these cookies, the Tool enables unique users identification (UUID) over browsing sessions, but the Tool cannot identify unique users in different browsers or devices. If a site owner's website has its own authentication system, the site owner can use the ID feature to identify a user more accurately on all the devices and browsers they use to access the site. When the information is collected, it is transferred to the servers of the Tool. All data collected through the Tool is stored in the United States.

Google has put in place, among other things, the following legal, organisational and technical measures to regulate transfers of data within the framework of the Tool.

Google has put in place legal and organisational measures, such as that it always conducts a thorough review of a request for access from government authorities if user data can be implemented. It is lawyers/specially trained staff who conduct these trials and investigate whether such a request is compatible with applicable laws and Google's guidelines. Data subjects are informed of the disclosure, unless prohibited by law or would adversely affect an emergency. Google has also published a policy on its website on how to implement such a request for access by government authorities of user data.

Google has put in place technical measures such as protecting personal data from interception when transmitting data in the Tool. By default using HTTP Strict Transport Security (HSTS), which instructs browsers such as http to SSL (HTTPS) to use an encryption protocol for all communication between end-users, websites, and tool servers. Such encryption prevents intruders from passively listening by communications between websites and users.

Google also uses encryption technology to protect personal data known as "data at rest" in data centers, where user data is stored on a disk or backup media to prevent unauthorised access to the data.

In addition to the above actions, website owners may use IP anonymisation by using the settings provided by the Tool to restrict Google's use of personal data. Such settings include, in particular, enabling IP anonymisation in the code of the Tool, which means that IP addresses are truncated and contribute to data minimisation. If the IP anonymisation service is fully used, the anonymisation of the IP address takes place almost immediately after the request has been received.

Google also restricts access to the data from the Tool through permission control and by all personnel having completed information security training.

1.5 CDON's comment on Google's opinion

CDON maintains what was stated in the opinion of 15 January 2021. In addition, CDON presents the following in response to Google's opinion of 9 April 2021.

In its use of the Tool, CDON has taken the security measures provided by the Tool.

Google's observations state, inter alia, as follows:

> *"As a general matter, unless instructed to do so, Google does not attempt to link data it collects as a processor on behalf of website owners using Google Analytics with data it collects as a controller in relation to its users and the relevant policies and systems are designed to avoid such linking."*

Google thus states that the owner of the website has full control over the personal data processed by Google by allowing users of the tool to provide Google with specific instructions to link the personal data with users. CDON has not given Google any such instructions.

CDON has instead focused on using the settings provided by the Tool to restrict Google's use of personal data. Such settings include, in particular, enabling IP anonymisation in the code of the Tool, which means that IP addresses are truncated. CDON had also limited the storage time of the personal data and has not enabled the User ID function. CDON has thus not been able to link a fixed ID of a single user to the user's engagement data from one or more sessions initiated from one or more devices.

In conclusion, CDON maintains that the use of the Tool has been carried out in accordance with the security measures offered by the Tool. It should also be noted that obligations under Chapter V of the GDPR are primarily obligations imposed on the exporter, which in this case are CDON resellers (see EDPB Guidelines 05/2021 and decisions of the data protection authority in Austria regarding Google Analytics in case 2021-0.586.257 (D155.027)).

2 Statement of reasons for the decision

2.1 The framework for the audit

Based on the complaint in the case, IMY has only examined whether CDON transfers personal data to the third country USA within the framework of the Tool and whether CDON has legal support for it in Chapter V of the GDPR. The supervision does not cover whether CDON's personal data processing otherwise complies with the General Data Protection Regulation.

2.2 This is the processing of personal data

2.2.1 Applicable provisions, etc.

In order for the GDPR to apply, personal data must be processed.

According to Article 1(2), the GDPR aims to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data. According to Article 4(1) of the GDPR personal data' *means 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".* In order to determine whether a natural person is identifiable, account should be taken of all means which, either by the controller or by another person, may reasonably be used to directly or indirectly identify the natural person (recital 26 of the GDPR).

That concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject. As regards the latter condition, it is satisfied where the information, by reason of its content, purpose or effect, is linked to a particular person.[7]

The word "indirectly" in Article 4(1) of the GDPR suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified.[8] In addition, recital 26 of the GDPR states that in order to determine whether a natural person is identifiable, any means, such as 'singling out', which, either by the controller or by another person, may reasonably be used to directly or indirectly identify the natural person, should be taken into account. In order to determine whether devices *may reasonably be used to* identify the natural person, all objective factors, such as the cost and duration of identification, taking into account both the available technology at the time of processing, should be taken into account. According to Article 4 (5) of the GDPR, 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

So-called "net identifiers" (sometimes referred to as "online identifiers") — e.g. IP addresses or information stored in cookies — can be used to identify a user, especially when combined with other similar types of information. According to recital 30 of the GDPR, natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as IP addresses, cookies or other identifiers. This may leave traces that, in particular in combination with unique identifiers and other data collected, can be used to create profiles of natural persons and identify them.

In its Breyer judgment, the Court of Justice of the European Union held that a person is not regarded as identifiable by a particular indication of whether the risk of

[7] Judgment of the Court of Justice of the European Union Nowak, C-434/16, EU:2017:994, paragraphs 34-35.
[8] Judgment of the Court of Justice of the European Union Breyer, C-582/14, EU:2016:779, para. 41.

identification is in practice negligible, which is whether the identification of the person concerned is prohibited by law or impossible to implement in practice.[9] However, in the judgment in M.I.C.M. of 2021 and in the Breyer judgment, the Court of Justice of the European Union held that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.[10]

2.2.2 Assessment of the Swedish Authority for Privacy Protection (IMY)
In order to determine whether the data processed through the Tool constitute personal data, IMY shall decide whether Google or CDON, through the implementation of the Tool, can identify individuals, e.g. the complainant, when visiting the Website or whether the risk is negligible.[11]

IMY considers that the data processed constitute personal data for the following reasons.

The investigation shows that CDON implemented the Tool by inserting a JavaScript code (a tag), as specified by Google, into the source code of the Website. While the page loads in the visitor's browser, the JavaScript code is loaded from Google LLC's servers and runs locally in the visitor's browser. A cookie is set simultaneously in the visitor's browser and stored on the computer. The cookie contains a text file that collects information about the visitor's operation on the Website. Among other things, a unique identifier is set in the value of the cookie and this unique identifier is generated and managed by Google.

When the complainant visited the Website, or a subpage of the Website, the following information was transmitted via the JavaScript code from the complainant's browser to Google LLC's servers:

1. Unique identifier(s) that identified the browser or device used to visit the Website and a unique identifier that identified CDON (i.e. the CDON account ID for Google Analytics).
2. URL and HTML title of the website and web page visited by the complainant;
3. Information about browser, operating system, screen resolution, language setting, and date and time of access to the Website.
4. The complainant's IP address.

At the time of the complainant's visit, the identifiers referred to in paragraph 1 above were set in cookies with the names '_gads', '_ga' and '_gid' and subsequently transferred to Google LLC. Those identifiers were created with the aim of distinguishing individual visitors, such as the complainant. The unique identifiers thus make visitors to the Website identifiable. However, even if such unique identifiers (according to 1 above) were not in themselves to make individual identifiable, it must be borne in mind that, in the present case, those unique identifiers may be combined with additional elements (according to paragraphs 2 to 4 above) and that it is possible

[9] Judgment of the Court of Justice of the European Union Breyer, C-582/14, EU:2016:779, paragraphs 45-46.
[10] Judgment of the Court of Justice of the European Union M.I.C.M, C-597/19, EU:2021:492, para. 102-104, and Breyer, C-582/14; EU:C:2016:779, paragraph 49.
[11] See the Administrative Court of Appeal in Gothenburg's judgment of 11 November 2021 in case No 2232-21, with the agreement of the lower court.

to draw conclusions in relation to information (as set out in paragraphs 2 to 4 above) from which data constitute personal data, irrespective of whether the IP address was not transmitted in its entirety.

Combined data (according to points 1-4 above) means that individual visitors to the Website become even more separable. It is therefore possible to identify individual visitors to the Website. This in itself is sufficient for it to be considered personal data. Knowledge of the actual visitor's name or physical address is not required, as the distinction (by the word 'release' in recital 26 of the GDPR, 'singling out' in the English version) is sufficient in itself to make the visitor indirectly identifiable. Nor is it necessary for Google or CDON to identify the complainant, but the possibility of doing so is in itself sufficient to determine whether it is possible to identify a visitor. *Objective means that can reasonably be used* either by the controller or by another, are *all means that can reasonably* be used for the purpose of identifying the complainant. Examples of *objective means that can reasonably be used* are access to additional information from a third party that would allow the complainant to be identified taking into account both the available technology at the time of identification and the cost (time required) of the identification.

IMY notes that, in its judgments in M.I.C.M. and Breyer, the Court of Justice of the European Union held that dynamic IP addresses constitute personal data in relation to the person processing them, where it also has a legal means to identify the holders of internet connections using the additional information available to third parties.[12] IP addresses do not lose their character of being personal data simply because the means of identification lie with third parties. The Breyer judgment and the M.I.C.M. judgment should be interpreted on the basis of what is actually stated in the judgments, i.e. if there is a lawful possibility of access to additional information for the purpose of identifying the complainant, it is objectively clear that there is a '*legal means which enable it'* to identify the complainant. According to IMY, the judges should not be read in contrast, in such a way as to demonstrate a legally regulated possibility of access to data that could link IP addresses to natural persons in order for the IP addresses to be considered personal data. In IMY's view, an interpretation of the concept of personal data which implies that there must always be a *legal possibility* of linking such data to a natural person would constitute a significant restriction on the area of protection of the Regulation and would open up the possibility of circumventing the protection provided for in the Regulation. That interpretation would, inter alia, run counter to the objective of the Regulation as set out in Article 1(2) of the GDPR. The Breyer judgment is decided under Directive 95/46 previously in force and the notion of 'singling out' as set out in recital 26 of the current regulation (not requiring knowledge of the actual visitor's name or physical address, since the distinction itself is sufficient to make the visitor identifiable), was not mentioned in the previous directives as a means of identifying personal data.

In this context, there are also other data (according to paragraphs 1 to 3 above) with which the IP address can be combined to enable identification. Google's action regarding[13] the truncation of an IP address means that the IP address can still be

---

[12] Judgment of the Court of Justice of the European Union M.I.C.M, C-597/19, EU:2021:492, para. 102-104 and Breyer, C-582/14
EU:C:2016:779, paragraph 49.

[13] Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255), which in itself can only be any of 256 options. The effect of this action means that it is still possible to distinguish the IP address from the other IP addresses (255 options), as he IP address can be linked with other transmitted data (e.g. information on the entity and time of visit) to third countries.

distinguished as it can be linked to other data transmitted to third countries (to the United States). This enables identification, which in itself is sufficient for the data to constitute personal data together.

In addition, several other supervisory authorities in the EU/EEA have decided that the transfer of personal data to third countries has taken place in the use of the Tool because it has been possible to combine IP addresses with other data (according to paragraphs 1 to 3 above), thus enabling the separation of data and the identification of the IP address, which in itself is sufficient to determine the processing of personal data.[14]

IMY notes that there may also be reasons to compare IP addresses with pseudonymised personal data. In accordance with Article 4(5) of the GDPR, pseudonymisation of personal data means that the data — like dynamic IP addresses — can no longer be attributed to a specific data subject without the use of additional information. According to recital 26 of the GDPR, such data should be considered to be data relating to an identifiable natural person.

According to IMY, a narrower interpretation of the concept of personal data would undermine the scope of the right to the protection of personal data, as guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, as it would allow controllers to specifically designate individuals together with personal data (e.g. when they visit a particular website) while denying individuals the right to protection against the dissemination of such data. Such an interpretation would undermine the level of protection of individuals and would not be compatible with the broad scope of the data protection rules laid down in the case-law of the Court of Justice of the European Union.[15]

Furthermore, CDON, by being logged in to its Google account when visiting the Website, processed data from which it was able to draw conclusions about the individual on the basis of his registration with Google. Google's opinion shows that the implementation of the Tool on a website makes it possible to obtain information that a user of a Google account (i.e. a data subject) has visited the website in question. It is true that Google states that certain conditions must be met in order for Google to receive such information, such as that the user (applicant) has not disabled the processing and display of personal ads. Since the applicant was logged in to its Google account when visiting the Website, Google may still have been able to obtain information about the logged-in user's visit to the Website. The fact that it is not apparent from the complaint that no personalised ads have been displayed does not mean that Google cannot obtain information about the logged-in user's visit to the Website.

In the light of the unique identifiers CAPABILITY of identifying the browser or device, the ability to derive the individual through its Google account, the dynamic IP addresses and the possibility of combining these with additional data, CDON's use of the Tool on a website, means the processing of personal data.

---

[14] Decision of the Austrian Supervisory Authority (Datenschultzbehörde) of 22 April 2022 concerning complaints Google Analytics represented by NOYB with local case number 1354838270, the French Supervisory Authority (CNIL) decision of 10 February 2022 represented by NOYB and the Italian Supervisory Authority (Garante) decision of 9 June 2022 concerning complaints Google Analytics represented by NOYB, local case number 9782890.
[15] See, for example, Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:2021:504, paragraph 61; Nowak, C-434/16, EU:2017:994, paragraph 33; and Rijkeboer, C-553/07, EU:2009:293, paragraph 59.

2.3 CDON is the data controller for the processing

The controller is, among other things, the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data (Article 4(7) GDPR). The processor is, among other things, a legal person who processes personal data on behalf of the controller (Article 4(8) GDPR).

The responses provided by CDON indicate that CDON has made the decision to implement the Tool on the Website. It also appears that CDON's purpose was to enable the company to analyse how the Website is used, in particular to be able to monitor the use of the website over time.

IMY finds that CDON, by deciding to implement the Tool on the Website for that purpose, has determined the purposes and means of the collection and subsequent transfer of this personal data. CDON is therefore the data controller for this processing.

2.4 Transfer of personal data to third countries

The investigation shows that the data collected through the Tool is stored by Google LLC in the United States. Thus, the personal data collected through the Tool is transferred to the United States.

The question is therefore whether CDON's transfer of personal data to the United States is compatible with Article 44 of the GDPR and has legal support for it in Chapter V.

2.4.1 Applicable provisions, etc.

Article 44 of the GDPR, entitled 'General principle for the transfer of data', provides, inter alia, that transfers of personal data which are under processing or are intended to be processed after their transfer to a third country — i.e. a country outside the EU/EEA — may take place only if, subject to the other provisions of the GDPR, the controller and processor fulfil the conditions set out in Chapter V. All provisions of that chapter are to be applied in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.

Chapter V of the GDPR contains tools that can be used for transfers to third countries to ensure a level of protection that is essentially equivalent to that guaranteed within the EU/EEA. This could include, for example, transfers based on an adequacy decision (Article 45) and transfers subject to appropriate safeguards (Article 46). In addition, there are derogations for specific situations (Article 49).

In Schrems II, the Court of Justice of the European Union annulled the adequacy decision previously in force in respect of the United States.[16] In the absence of an adequacy decision since July 2020, transfers to the United States cannot be based on Article 45 of the GDPR.

Article 46(1) provides of the GDPR, inter alia, that in the absence of a decision in accordance with Article 45(3), a controller or processor may only transfer personal data to a third country after having taken appropriate safeguards, and subject to the

[16] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Privacy Shield of the European Union and the United States and the judgment of the Court of Justice of the European Union Facebook Ireland and Schrems (Schrems II), C-311/18, EU:C:2020:559.

availability of statutory rights of data subjects and effective remedies for data subjects. Article 46(2)(c) provides that such appropriate safeguards may take the form of standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).

In Schrems II, the Court of Justice did not reject standard contractual clauses as a transfer tool. However, the Court found that they are not binding on the authorities of the third country. In that regard, 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.*'[17]

The reason why the Court of Justice of the European Union annulled the adequacy decision with the US was how the U.S. intelligence agencies can access personal data. According to the Court of Justice, the conclusion of standard contractual clauses cannot in itself ensure a level of protection required by Article 44 of the GDPR, as the safeguards set out therein do not apply when such authorities request access. The Court of Justice of the European Union therefore stated:

> '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'.*[18]*

The recommendations of the European Data Protection Board (EDPB) on the consequences of the judgment[19] clarify that if the assessment of the law and practice of the third country means that the protection guaranteed by the transfer tool cannot be maintained in practice, the exporter must, in the context of his transfer, as a rule either suspend the transfer or take appropriate supplementary measures. In that regard, the EDPB notes that '*Any supplementary measure may only be deemed effective in the meaning of the CJEU judgment "Schrems II" if and to the extent that it - by itself or in combination with others - addresses the specific deficiencies identified in your assessment of the situation in the third country as regards its laws and practices applicable to your transfer. If, ultimately, you cannot ensure an essentially equivalent level of protection, you must not transfer the personal data*.'[20]

---

[17] Points 125-126.
[18] Paragraph 133.
[19] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, adopted on 18 June 2021 (hereinafter "EDPB Recommendations 01/2020").
[20] EDPB Recommendations 01/2020, item 75.

The recommendations of the EDPB show that such supplementary measures can be divided into three categories: contractual, organisational and technical.[21]

As regards *contractual* measures, the EDPB states that such measures "*In some situations, these measures may complement and reinforce the safeguards the transfer tool and relevant legislation of the third country" [...]. Provided the nature of contractual measures, generally not capable of binding the authorities of that third country when they are not party to the contract, these measures may often need to be combined with other technical and organisational measures to provide the level of data protection required [...]'.*[22]

With regard to *organisational* measures, the EDPB stresses*"[a] electing 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 assessment performed on the legislation of the third country, organisational measures are needed to complement contractual and/or technical measures, in order to ensure a level of protection of the personal data essentially equivalent to that guaranteed within the EEA*".[23]

With regard to *technical* measures, the EDPB points out that *'measures, which may supplement safeguards found in Article 46 GDPR transfer tools to ensure compliance with the level of protection required under EU law in the context of a transfer of personal data to a third country'*.[24] The EDPB states in this regard that *" The measures listed below 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.79 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*".[25]

2.4.2 Assessment of the Swedish Authority for Privacy Protection (IMY)

2.4.2.1 Applicable transfer tool

The investigation shows that CDON and Google have entered into standard data protection clauses (standard contractual clauses) within the meaning of Article 46 for the transfer of personal data to the United States. These clauses are in line with those published by the European Commission in Decision 2010/87/EU and thus a transfer tool under Chapter V of the GDPR.

---

[21] EDPB Recommendations 01/2020, item 52.
[22] EDPB Recommendations 01/2020, item 99.
[23] EDPB Recommendations 01/2020, item 128.
[24] EDPB Recommendations 01/2020, item 77.
[25] EDPB Recommendations 01/2020, item 79.

2.4.2.2 Legislation and situation in the third country

As can be seen from the judgment in Schrems II, the use of standard contractual clauses may require supplementary measures. Therefore, an analysis of the legislation of the third country in question needs to be carried out.

IMY considers that the analysis already carried out by the Court of Justice of the European Union in Schrems II, which relates to similar circumstances, is relevant and topical, and that it can therefore serve as a basis for the assessment in the case without further analysis of the legal situation in the United States.

Google LLC, as an importer of the data to the United States, shall be classified as an electronic communications service provider within the meaning of 50 US Code § 1881(b)(4). Google is therefore subject to surveillance by U.S. intelligence agencies pursuant to 50 US § 1881a ("702 FISA") and is therefore obliged to provide the U.S. government with personal data when 702 FISA is used.

In Schrems II, the Court of Justice of the European Union held that the US surveillance programmes based on 702 FISA, Executive Order 12333 (hereinafter 'E.O. 12333') and Presidential Policy Directive 28 (hereinafter 'PPD-28') do not meet the minimum requirements laid down in EU law in accordance with the principle of proportionality. This means that the monitoring programmes based on those provisions cannot be considered to be limited to what is strictly necessary. In addition, the Court found that the monitoring programmes do not confer rights on data subjects that may be invoked against US authorities in court, which means that those persons do not have the right to an effective remedy.[26]

Against this background, IMY notes that the use of the European Commission's standard contractual clauses is not in itself sufficient to achieve an acceptable level of protection for the transferred personal data.

2.4.2.3 Supplementary measures implemented by Google and CDON

The next question is whether CDON has put in place supplementary measures.

As the controller and exporter of the personal data, CDON is obliged to ensure compliance with the rules of the GDPR. This responsibility includes, inter alia, assessing, on a case-by-case basis, in the case of transfers of personal data to third countries, which supplementary measures are to be used and to what extent, including assessing whether the measures taken together by the recipient (Google) and the exporter (CDON) are sufficient to achieve an acceptable level of protection.

2.4.2.3.1 Google's supplementary measures

Google LLC, as an importer of personal data, has taken contractual, organisational and technical measures to supplement the standard contractual clauses. In its opinion of 9 April 2021, Google stated that it had taken action.

The question is whether the supplementary measures taken by CDON and Google LLC are effective, in other words, hindering the ability of U.S. intelligence agencies to access the transferred personal data.

---

[26] Paragraphs 184 and 192. Paragraph 259 et seq.

As regards the *legal and organisational measures, it* can be noted that neither information to users of the Tool (such as CDON), the[27] publication of a transparency report or a publicly available *"government enquiries policy*" prevents or reduces the ability of U.S. intelligence services to access the personal data. In addition, it is not described what it means that Google LLC's "*scrupulous review" of any "legality" request* from U.S. intelligence agencies. IMY notes that this does not affect the legality of such requests as, according to the CJEU, they are not compatible with the requirements of EU data protection rules.

As regards the *technical measures* taken, neither Google LLC nor CDON have clarified how the described measures — such as the protection of communications between Google services, the protection of data when transferring between data centres, the protection of communications between users and websites, or "physical security" — prevent or reduce the ability of U.S. intelligence services to access the data under the US regulatory framework.

With regard to the encryption technology used — for example, for so-called "data at rest" ("data at rest") in data centers, which Google LLC mentions as a technical measure — Google LLC as an importer of personal data nevertheless has an obligation to grant access to or supply imported personal data held by Google LLC, including any encryption keys necessary to make the data understandable.[28] Thus, such a technical measure cannot be considered effective as long as Google LLC is able to access the personal data in plain language.

As regards Google LLC's argument that *'to the extent that data for measurement in Google Analytics transmitted by website holders constitute personal data, they may be regarded as pseudonymised', it can be* concluded that Universal Unique Identifiers (UUIDs) are not covered by the concept of pseudonymisation in Article 4(5) of the GDPR. Pseudonymisation can be a privacy-enhancing technology, but the unique identifiers, as described above, have the specific purpose of distinguishing users and not serving as protection. In addition, individual identification is made through what has been stated above about the ability to combine unique identifiers and other data (e.g. metadata from browsers or devices and the IP address) and the ability to link such information to a Google account for logged-in users.

In the case of Google's "anonymisation of IP addresses" in the form of truncation[29], Google's response does not indicate whether this action takes place prior to transmission, or whether the full IP address is transmitted to the United States and shortened only after transmission to the United States. From a technical point of view, it has therefore not been shown that there is no potential access to the entire IP address before the last octet is truncated.

Against this background, IMY concludes that the supplementary measures put in place by Google are not effective, as they do not prevent US intelligence services from accessing the personal data or rendering such access ineffective.

---

[27] Regardless of whe her such a notification would even be permitted under U.S. law.
[28] See EDPB Recommendations 01/2020, paragraph 81.
[29] Truncation of IP address means that asterisks or zeros replace other digits in he last octets (last digits of an IP address, a number between 0 and 255).

2.4.2.3.2 CDON's own supplementary measures

CDON has stated that it has taken supplementary measures in addition to the measures taken by Google. According to the CDON,these consist of activating the function of truncating[30] the last octet of the IP address before the data is transmitted to Google, which means that the last octet is masked.[31]

As stated above with regard to Google's actions, it is not apparent from Google's reply whether this action takes place prior to transmission or whether the full IP address is transmitted to the United States and truncated only after the transfer to the United States. Therefore, from a technical point of view, it has not been established that, after the transmission, there is no potential access to the entire IP address before the last octet is truncated.

Even if the truncation were to take place before the transfer, it is not a sufficient measure, as the truncated IP address can be linked to other data, as IMY stated above in section 2.2.2. A truncation of an IP address means that only the last octet is masked, which in itself can only be any of 256 options (i.e. in the range 0-255) and because the truncated IP address can be distinguished from other IP addresses, this data can be linked to other data (as described in section 2.2.2) and enable identification, which is sufficient in itself to determine whether the data is a personal data. Although the masking of the last octet constitutes a privacy-enhancing measure, as it limits the scope of the data that authorities can access (in third countries), IMY notes that it is nevertheless possible to link the transferred data to other data which are also transferred to Google LLC (in third countries).

Against this background, IMY also notes that the supplementary measures taken by CDON in addition to the supplementary measures taken by Google are not effective enough to prevent US intelligence services from accessing the personal data or rendering such access ineffective.

2.4.2.3.3 Conclusion of the Swedish Authority for Privacy Protection (IMY)

IMY finds that CDON and Google's actions are neither individually nor collectively effective enough to prevent U.S. intelligence services from accessing the personal data or rendering such access ineffective.

Against this background, IMY considers that neither standard contractual clauses nor the other measures relied on by CDON can support the transfer as set out in Chapter V of the GDPR.

With this transfer of data, CDON therefore undermines the level of protection of personal data for data subjects guaranteed by Article 44 of the GDPR.

IMY therefore concludes that CDON AB violates Article 44 of the GDPR.

---

[30] Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255).
[31] See above in the section on CDON's submissions, under the heading 'Supplementary protective measures taken'.

3 Choice of intervention

3.1 Legal regulation

In case of breaches of the GDPR, IMY has a number of corrective powers available under Article 58(2)(a) to (j) of the GDPR, including reprimand, injunctions and administrative fines.

IMY shall impose fines in addition to or in place of other corrective measures referred to in Article 58(2), depending on the circumstances of each case.

Each supervisory authority shall ensure that the imposition of administrative fines on a case-by-case basis is effective, proportionate and dissuasive. This is set out in Article 83(1) of the GDPR.

Article 83(2) of the GDPR sets out the factors to be taken into account in determining whether an administrative fine is to be imposed, but also in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand under Article 58(2)(b) of the Regulation. Account must be taken of aggravating and mitigating circumstances in the case, such as the nature, gravity and duration of the infringement and the relevant past infringements.

The EDPB has adopted guidelines on the calculation of administrative fines under the GDPR, which aim to create a harmonised methodology and principles for the calculation of fines.[32]

3.2 Should an administrative fine be imposed?

IMY has found above that the transfers of personal data to the United States carried out through the Google Analytics tool and for which CDON is responsible are contrary to Article 44 of the GDPR. Infringements of that provision may, in accordance with Article 83, impose fines.

Given, among other things, that CDON has transferred a large amount of personal data, that the processing has been going on for a long time and that the transfer has meant that the personal data could not be guaranteed the level of protection afforded in the EU/EEA, this is not a minor breach. A fine must therefore be imposed on CDON for the infringement found. See also below under 3.3 for a detailed description of the gravity of the infringement.

3.2.1 To what amount should the administrative fine be determined to?

In determining the maximum amount of a fine to be imposed on an undertaking, the definition of 'undertaking' used by the Court of Justice of the European Union for the purposes of Articles 101 and 102 TFEU (see recital 150 of the GDPR). It is clear from the Court's case-law that this applies to any entity engaged in an economic activity, irrespective of its legal form and the way in which it is financed, and even if, in the legal sense, the entity consists of several natural or legal persons.[33]

[32] EDPB Guidelines 8/2020 Guidelines 04/2022 on the calculation of administrative fines under the GDPR.
[33] See judgment in Akzo Nobel, C-516/15, EU:C:2017:314, paragraph. 48

Pursuant to Article 83(5)(c) GDPR, in the event of infringement of, inter alia, Article 44 in accordance with 83(2), administrative fines of up to EUR 20 million or, in the case of an undertaking, up to 4 % of the total global annual turnover in the preceding financial year, whichever is higher, are to be imposed.

IMY considers that the company's turnover to be used as a basis for calculating the administrative fine is CDON's annual report for 2022. The company had sales of approximately SEK 461 000 000 during that financial year. This amount is less than EUR 20 million and the administrative fine can therefore be set at an amount of up to EUR 20 million.

In determining the amount of the fine, IMY shall determine, having regard to the gravity of the infringement and taking into account both aggravating and mitigating factors, an administrative fine amount which is effective, proportionate and dissuasive in the individual case.

IMY considers that the following factors are relevant to the assessment of the gravity of the infringement.

As far as the assessment of the gravity of the infringement is concerned, there are, at the outset, factors that lead to a more serious assessment of the infringement. CDON is transferring a large amount of personal data to third countries. The transfer has meant that the personal data have not been guaranteed the level of protection afforded in the EU/EEA, which in itself is a serious breach. In addition, it is aggravating that the transfer of personal data has been going on for a long time, i.e. from 14 August 2020 and is still ongoing, and that it has taken place systematically. IMY also takes into account that it has now elapsed around 3 years since the Court of Justice of the European Union, by judgment of 16 July 2020, rejected the Commission's adequacy decision in the United States,[34] thereby changing the conditions for transfers of personal data to the United States.

In the meantime, the EDPB made recommendations on the consequences of the judgment that had been out for public consultation on 10 November 2020 and adopted in final form on 18 June 2021. In addition, several other EU/EEA supervisory authorities have issued injunctions to discontinue the use of the Tool until sufficiently effective security measures have been taken by the controllers. The decisions have covered cases where the controllers have also taken measures such as the "anonymisation of IP addresses" in the form of truncation.[35]

Although these recommendations and decisions clearly point to the risks and difficulties of ensuring an adequate level of protection for data transfers to U.S. companies, CDON has not put in place supplementary measures of its own. Google's[36] IP truncation action means that the IP address can still be distinguished as

[34] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield.
[35] Decision of the Austrian Supervisory Authority (Datenschultzbehörde) of 22 April 2022 concerning complaints Google Analytics represented by NOYB with local case number 1354838270, the French Supervisory Authority (CNIL) decision of 10 February 2022 represented by NOYB and the Italian Supervisory Authority (Garante) decision of 9 June 2022 concerning complaints Google Analytics represented by NOYB, local case number 9782890.
[36] Truncation of IP address "anonymisation of IP address" means hat asterisks or zeros replace other digits in last octets (last digits of an IP address, a number between 0 and 255), which in itself can only be any of 256 options. The effect of this measure means that it is still possible to distinguish the IP address from the other IP addresses (255 options), as the IP address can be linked wi h other transmitted data (e.g. information about the entity and time of visit) to third countries (to the USA).

it can be linked to other data transmitted to third countries (to the United States). This enables identification, which means that the data together constitute personal data.

The CDON website is also a well-attended e-commerce portal that offers goods from many different suppliers and is available in several countries and in several languages. These are data on a large number of data subjects in the EU/EEA that can be identified indirectly and whose data can be linked to other data relating to them. As regards the nature of the data, it follows from CDON's own purpose of processing — i.e. to be able, inter alia, to draw conclusions on how data subjects navigate and find the Website, that the data taken together make it possible to draw relatively precise conclusions about the privacy of data subjects and to map them, such as what they buy and which goods they are interested in over time. CDON´s analysis of the Tool shows that the company have a proposal for a solution other than the Tool, but the company has chosen not to introduce this solution due to the fact that such a change would be particularly burdensome for the company. CDON´s processing of personal data entails obvious risks of serious violation of the rights and freedoms of individuals, which gives CDON a special responsibility which imposes high standards in the case of transfers to third countries, where IMY overall considers that CDON has not demonstrated that it has carried out sufficient analysis and mapping, nor has it taken the necessary security measures to limit the risks to the data subjects.

At the same time, IMY notes that there are factors that speak in the opposite direction. IMY takes into account the specific situation arising after the judgment and the interpretation of the EDPB's recommendations, where there has been a gap after the transfer tool to the United States has been rejected by the Court of Justice of the European Union, according to the Commission's previous decision. IMY also takes into account that CDON has taken some, albeit insufficient, measures to restrict the personal data transmitted by activating the "anonymisation of IP addresses" by truncation.[37] That fact is also taken into account when assessing the gravity of the infringements.

Overall, considering the facts set out in this decision, IMY considers that the infringements in question are of a low degree of seriousness. The starting point for calculating the fine should therefore be set low in relation to the maximum amount in question. In order to ensure a proportionate fine in the individual case, it is also necessary, at this stage, to further adjust the starting point for the further calculation downward, taking into account the high turnover underlying the calculation of the fine.

In addition to assessing the gravity of the infringement, IMY shall assess whether there are any aggravating or mitigating circumstances that have a bearing on the amount of the fine. IMY considers that there are no additional aggravating or mitigating circumstances, other than those taken into account when assessing the severity, which affect the amount of the fine.

On the basis of an overall assessment of the above facts and in the light of the fact that the administrative fine must be effective, proportionate and dissuasive, IMY considers that the fine may remain at SEK 300 000 (three hundred thousand).

---

[37] Decision of the Austrian Supervisory Authority (Datenschultzbehörde) of 22 April 2022 concerning complaints Google Analytics represented by NOYB with local case number 1354838270, the French Supervisory Authority (CNIL) decision of 10 February 2022 represented by NOYB and the Italian Supervisory Authority (Garante) decision of 9 June 2022 concerning complaints Google Analytics represented by NOYB, local case number 9782890.

3.3 Other interventions

Against this background IMY considers that CDON should be ordered pursuant to Article 58(2)(d) of the GDPR to ensure that its processing of personal data in the context of its use of the Google Analytics tool complies with Article 44 and the other provisions of Chapter V. In particular, by discontinuing the use of the version of the Google Analytics tool used on 14 August 2020, unless appropriate safeguards are in place. The measures shall be implemented no later than one month after the date of entry into force of this Decision.

4 How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection. Please indicate in your letter the decision you want to appeal and the amendment that you are requesting. The appeal must reach the Swedish Authority for Privacy Protection no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can send the appeal by e-mail to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. The Swedish Authority for Privacy Protection's contact details are set out in the first page of the decision.

This decision was taken by Director-General [redacted] following a presentation by the legal advisor [redacted], Head of Legal Affairs, [redacted], Head of Unit and information security specialist [redacted] have also participated in the final proceedings.