Integritetsskydds myndigheten

CDON AB
Box 385
20123 Malmö

Document number:
DI-2020-11397

Date:
2023-06-30

Supervisory decision under the GDPR - CDON AB's transfer of personal data to third countries

Contents

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

Decision of the integrity protection authority

The Authority finds that CDON AB processes personal data in breach of Article 44 of the GDPR[1] by using, from 14 August 2020 until the date of this decision, the Google Analytics tool provided by Google LLC on its website www.cdon.fi, thereby transferring personal data to third countries without complying with the conditions laid down in Chapter V of the Regulation.

Pursuant to Article 58(2)(d) of the GDPR, the Swedish Data Protection Authority orders CDON AB to ensure that the company's processing of personal data within the framework of the company's use of the Google Analytics tool complies with Article 44 and the other provisions of Chapter V. This shall be done in particular by ceasing to use the version of the Google Analytics tool used on 14 August 2020. This shall be done in particular by CDON AB ceasing to use the version of the Google Analytics tool that was used on 14 August 2020, unless adequate safeguards have been taken. The measures must be implemented no later than one month after this decision becomes legally effective.

IMY decides, pursuant to Article 58(2) and 83 of the General Data Protection Regulation, that CDON AB shall pay an administrative fine of SEK 300,000 (three hundred thousand) for infringement of Article 44 of the General Data Protection Regulation.

1 Description of the supervision case

1.1 The organisation

The Swedish Data Protection Authority (IMY) has initiated supervision of CDON AB (hereinafter CDON or the company) following a complaint. The complaint concerns an alleged breach of the provisions of Chapter V of the GDPR linked 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 ("the company's website" or "the Website") through the Google Analytics tool ("the Tool") provided by Google LLC.

The complaint has been transferred to IMY, as the responsible supervisory authority under Article 56 of the GDPR. The transfer was made by the supervisory authority of the country where the complainant lodged the complaint (Austria) in accordance with the Regulation's provisions on co-operation in cross-border processing.

The processing at IMY has been carried out by correspondence. Given the cross-border nature of the processing, IMY has made use of the co-operation and consistency mechanisms provided for in Chapter VII of the GDPR. The supervisory authorities concerned have been the supervisory authorities of Germany, Norway, Estonia, Denmark, Portugal, Spain, Finland and Austria.

1.2 What is stated in the complaint

The complaint essentially states the following.

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

On 14 August 2020, the complainant visited CDON's website. During the visit, the complainant was logged in to his Google account, which is linked to the complainant's email address. CDON had implemented on its website a Javascript code for Google's services, including Google Analytics. In accordance with point 5.1.1(b) of the New Order Data Processing Conditions for Google Advertising Products, Google processes personal data on behalf of the data controller (i.e. CDON) and should therefore be classified as its processor.

While visiting the company's website, CDON processed the complainant's personal data, at least the complainant's IP address and data collected through cookies. Some of the data has been transferred to Google. In accordance with paragraph 10 of the terms and conditions regarding the processing of personal data for Google's advertising products, CDON has authorised Google to process the complainant's personal data in the United States. Such transfer of data requires a legal basis in accordance with Chapter V of the GDPR.

According to the CJEU judgment in Facebook Ireland and Schrems (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 US. CDON should not base the transfer of data on standardised data protection clauses under Art.
46(2)(c) of the GDPR if the recipient country does not ensure an adequate level of protection under Union law for the personal data transferred.

Google is to be classified as a provider of electronic communications services within the meaning of 50 US Code § 1881 (4)(b) and is thus subject to surveillance by US intelligence agencies pursuant to 50 US § 1881a (section 702 of the Foreign Intelligence Surveillance Act, hereinafter '702 FISA').[3] Google provides the US government with personal data in accordance with those provisions.
Therefore, CDON cannot ensure adequate protection of the complainant's personal data when it is transferred to Google.

1.3 What CDON has stated

In its statements of 15 January 2021, 15 February 2022 and 31 August 2022, CDON AB mainly stated the following.

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

The code of 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 taken by CDON, a company registered in Sweden. Data is collected from all persons visiting the Website, which is likely to include data subjects from more than one EU/EEA Member State.

CDON uses the Tool to learn about traffic and uses the Website to make various business-critical decisions. For example, with the help of the Tool it is possible to find out which product categories are most popular and how customers navigate, both to find CDON and to complete a purchase.

---

[2] CJEU judgment 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.

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 various characteristics or actions taken by the visitor on the website, such as:

1. What elements the user sees when navigating and looking around the Website,
2. Clicked on an image/banner on the Website,
3. Added or removed something from the shopping basket,
4. Arrived at the checkout or completed a purchase,
5. Clicked on suggested accessories on product pages or added something to the wish list,
6. If the user is a member of CDON's customer club, and
7. The search string used by the user to search internally on the Website.

In addition to this data, Google also receives the IP address of each user.

1.3.4 Categories of persons concerned by the processing
The categories of persons concerned by the processing are all categories of persons visiting the Website. CDON has no possibility to distinguish whether data on particularly vulnerable persons is 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 actual transfer of the information to Google. CDON cannot identify individual users either before or after disclosure to Google. Thus, CDON has no knowledge of which category of person a unique user belongs to.

1.3.5 When the code of the Tool is executed and access is granted to the recipient immediately after the Website has finished loading in the user's browser, information about the user's location on the Website is transmitted to Google.
Since 12 January 2021, CDON has activated a tool that means that the respective user's consent is required for the Tool's content to be integrated and run in the user's browser.

1.3.6 How long the personal data is stored
Data and other information is not stored by CDON but is transferred in real time from CDON to Google using the Tool. CDON's assessment is that the anonymisation of IP addresses described below means that the data transferred to Google can no longer be linked to a specific individual and is therefore not to be considered personal data. Google only stores personal data until the IP addresses have been truncated.[4] According to information from Google, truncation is carried out as soon as it is technically possible.

1.3.7 Which countries the personal data is processed in
The data transferred to the Tool is stored, inter alia, in the United States.

[4] IP address truncation means that asterisks or zeros replace other digits in last octets (last digits of an IP address, a

number between 0 and 255).

1.3.8 CDON's relationship with Google LLC
CDON shares the assessment made by Google regarding the allocation of personal data responsibility, which means that Google is considered to process data within the framework of CDON's use of the Tool as a data processor for CDON. CDON acts as a data controller.

The terms and conditions applicable to the Tool are the Google Terms of Use and the Google Data Processing Terms.

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

1.3.9 Ensuring that the processing does not take place for the recipients' own purposes CDON has not had reason to assume that Google does not fulfil the requirements of the aforementioned Google Ads Data Processing Terms, which is why Google's compliance with these 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 learn about the traffic on the Website and to be able to make various business-critical decisions based on this information. For example, with the help of the Tool it is possible to find out which product categories are most popular and how customers navigate the Website to find CDON and to complete a purchase.

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

On 26 October 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 responded to CDON's request for information and for this reason CDON has, in addition to repeating the request to Google and reminding it to respond, sought publicly available information on the measures taken by Google as a result of the decision.

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 transmission of JavaScript libraries and measurement data using the HTTP HSTS (Strict Transport Security) encryption protocol.
- The tool has been certified to the internationally accepted independent security standards ISO 27001.

In addition to these measures, CDON has also chosen to activate IP anonymisation in the code for the Tool, which means that IP addresses are truncated. IP anonymisation (truncation) means that the last octet in IPv4 addresses and the last 80 bits in IPv6 addresses are deleted immediately after the addresses have been sent to the collection network for the Tool. 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 is

of IP addresses means that no information transmitted to Google is considered personal data after the IP anonymisation/truncation has been carried out.

1.3.12 Transfer tools under Chapter V of the General Data Protection Regulation Transfers of personal data to recipients in third countries within the framework of 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 the Google Data Processing Terms in force since 12 August 2020, Google and CDON have entered into the EU Standard Contractual Clauses for the transfer of data from an EU controller to a non-EU processor, based on the European Commission's template 2010/87/EU.

1.3.13 Verification of obstacles to enforcement in third country legislation
In order to ensure that the contractual obligations in the standard contractual clauses are fulfilled, CDON has sent the request for information to Google regarding third country transfer described above and CDON has not received a response.

1.3.14 What information falls under 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, the 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 identifier(s) (which can be attributed to the browser or device (i.e. CDON's account ID for Google Analytics)) either alone or in combination with, among other things, the information generated when visiting the Website (i.e. CDON's account ID for Google Analytics).
CDON is of the firm opinion that IP addresses are necessary to, among other things, process the information generated when visiting the Website (i.e. web address (URL) and HTML title of that Website or browser information) to be considered personal data. CDON recognises that under certain circumstances dynamic IP addresses can be considered personal data. However, the differentiation of users made possible by the information collected by unique identifier(s) is not sufficient for a specific individual to be identified, with or without means such as e.g. thinning, but it is only in combination with a full IP address that the information collected by unique identifier(s) and information generated when visiting the Website may constitute personal data.

The Breyer[5] and M.I.C.M.[6] judgements support the assessment that dynamic IP addresses are to be regarded as personal data in all cases. According to the CJEU, dynamic IP addresses are to be regarded as personal data in relation to the relevant provider of information or communication services, not in relation to each actor who gains access to an IP address. In Breyer, concerning the assessment of the means which may reasonably be used to identify the person concerned, the Court held that, under German law, there were legal means enabling the provider of electronic information or communication services, in particular in the event of a cyber-attack, to approach the competent authority to take the necessary steps to obtain such information from the internet service provider and to initiate criminal proceedings. It is questionable whether a US authority with a truncated IP address, which can be one of 256 alternative IP addresses, has

[5] CJEU judgment Breyer, C-582/14, EU:C:2016:779.
[6] CJEU judgment M.I.C.M, C-597/19, EU:C:2021:492.

such lawful means as may reasonably be used to enable the identification of an individual, when in the Breyer case even a full IP address was considered problematic in relation to the actual provider of the natural person's IT services.

1.3.15 Effectiveness of protective measures taken by Google and CDON
With reference to the answers above, in addition to the activation of the IP anonymisation, CDON has not considered the implementation of additional 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 truncation of the IP addresses takes place before, in connection with, or in direct connection with the transfer of the information from CDON to Google. The truncation of the IP addresses means that the information stored on Google's servers in the USA does not constitute personal data. In a situation where the truncation is carried out only when the data has been received by Google LCC, but at the latest in direct connection with the receipt, the truncation means that all data that has been transferred by CDON to Google and that is stored on Google's servers will not constitute personal data because the IP address, which is the unique identifier that means that other transmitted information constitutes personal data, has been anonymised. The IP address without the last octet can be any of 256 alternatives IP addresses and therefore a truncated IP address, by means of screening, together with other information, *cannot be* considered as personal data.

1.3.16 Additional protective 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. Coop has
has made preparations for such a change, which the company hopes to be able to implement promptly in the event that IMY's final decision entails a finding that the Tool is not compatible with the General Data Protection Regulation and this gains legal force. It should be emphasised, however, that CDON's analysis shows that such a change will be very burdensome for the company (especially in comparison to other players in the market), which is why it cannot be implemented until there is clarity in relation to what applies to the Tool regarding what is a sufficient protection measure.

1.4 What Google LLC has stated

IMY has added to the file an opinion from Google LLC (Google) dated 9 April 2021, submitted by Google to the Austrian supervisory authority. The opinion responds to questions posed by IMY and a number of supervisory authorities to Google in relation to the partial joint handling of similar complaints received by those authorities. CDON has been given the opportunity to comment on Google's statement. Google's statement states 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. The Tool then performs the tracking operation, which consists of collecting information related to the call in various ways and sending the information to the Tool's servers.

A webmaster who has integrated the Tool on his website can send instructions to Google for the processing of the data collected. These instructions are transmitted via the so-called tag manager that manages the tracking code that the webmaster has integrated into his website and via the

the tag manager's settings. The integrator can make various settings, for example regarding the retention time. The tool also allows the integrator to monitor and maintain the stability of their website, for example by being informed of events such as peaks in visitor traffic or lack of traffic. The tool also allows a website manager to measure and optimise the effectiveness of advertising campaigns carried out using other Google tools.

In this context, the Tool collects the visitor's HTTP request and information about, inter alia, the visitor's browser and operating system. According to Google, an HTTP request for any page contains information about the browser and the device making the request, such as the domain name, and information about the browser, such as the 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 request. Through these cookies, the Tool enables the identification of unique users (UUID) across browsing sessions, but the Tool cannot identify unique users across browsers or devices. If a website owner's website has its own authentication system, the website owner can use the ID feature to more accurately identify a user across all the devices and browsers they use to access the website.
When the information is collected, it is transferred to the Tool's servers. All data collected through the Tool is stored in the United States.

Google has implemented, inter alia, the following legal, organisational and technical safeguards to regulate data transfers within the Tool.

Google has put in place legal and organisational safeguards such as always conducting a thorough assessment of the feasibility of a request for access to user data from government authorities. These assessments are carried out by lawyers/specialised staff who examine whether such a request is compatible with applicable laws and Google's policies. Data subjects are informed of the disclosure, unless it is prohibited by law or would adversely affect an emergency situation. Google has also published a policy on its website on how to implement such requests for access by government authorities to user data.

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

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

In addition to the above measures, website owners can use IP anonymisation by using the settings provided by the Tool to limit Google's use of personal data. Such settings include, in particular, enabling in the code of the Tool IP anonymisation, 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 occurs almost immediately after the request is received.

Google also restricts access to the data from the Tool through authorisation controls and by requiring all staff to undergo information security training.

1.5 CDON's comment on Google's statement

CDON maintains what was stated in its opinion of 15 January 2021. In addition, CDON makes the following points with regard 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 opinion states, inter alia, the following:

> *"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."*

Thus, Google argues that the owner of the website has full control over the personal data processed by Google because there is a possibility for users of the Tool to give Google specific instructions to associate 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 limit Google's use of personal data. Such settings include, above all, activating IP anonymisation in the code for the Tool, which means that IP addresses are truncated. CDON had also limited the storage time of the personal data and has not activated the User ID function. Thus, CDON has not been able to link a fixed ID for a single user to the user's engagement data from one or more sessions initiated from one or more devices.

In summary, CDON maintains that the use of the Tool has been 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 is CDON's retailer (see EDPB Guidelines 05/2021 and the decision of the Austrian data protection authority regarding Google Analytics in case 2021-0.586.257 (D155.027)).

2 Justification of the decision

2.1 The framework of 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 this in Chapter V of the GDPR. The supervision does not include whether CDON's personal data processing is otherwise compatible with the GDPR.

2.2 It is a matter of processing personal data

2.2.1 Applicable provisions, etc.
The application of the GDPR requires the processing of personal data.

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 Regulation, personal data are "*any information relating to an identified or identifiable natural person ('data subject'), an identifiable natural person being one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or online identifiers, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*". To determine whether a natural person is identifiable, account should be taken of any means likely to be used, either by the controller or by another person, to directly or indirectly identify the natural person (Recital 26 of the GDPR).

The concept of personal data can include any information, whether objective or subjective, provided that it 'relates' to a specific person, which it does if it is linked to that person by virtue of its content, purpose or effect.[7]

The word "indirectly" in Article 4(1) of the GDPR suggests that it is not necessary that the information itself makes it possible to identify the data subject in order for it to be personal data.[8] Furthermore, Recital 26 of the GDPR states that in order to determine whether a natural person is identifiable, any means, such as "singling out", which could reasonably be used, either by the controller or by another person, to directly or indirectly identify the natural person should be taken into account. In order to determine whether means are reasonably *likely to be used to* identify the natural person, all objective factors, such as the cost and time required for identification, taking into account both the technology available at the time of the processing, should be taken into account. Article 4(5) of the Regulation states that '*pseudonymisation' means the* processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of supplementary information, provided that such supplementary information is kept separately and is subject to technical and organisational measures ensuring that the personal data are not attributed to an identified or identifiable natural person.

So-called "online identifiers" (sometimes referred to as "online identifiers") - such as 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 can be linked to online identifiers provided by their equipment, such as IP addresses, cookies or other identifiers. This can leave traces which, especially in combination with unique identifiers and other data collected, can be used to profile and identify natural persons.

In Breyer, the CJEU ruled that a person is not considered identifiable through a particular piece of information if the risk of identification is negligible in practice, which it is if

[7] CJEU judgment Nowak, C-434/16, EU:C:2017:994, paragraphs 34-35.
[8] ECJ judgment Breyer, C-582/14, EU:C:2016:779, paragraph 41.

identification of the person concerned is prohibited by law or impossible to implement in practice.[9] However, in the 2021 M.I.C.M. judgment and in the Breyer judgment, the CJEU has recognised that dynamic IP addresses constitute personal data in relation to the data controller, where the latter also has the legal possibility of identifying the holders of the internet connections by means of the additional information held by third parties.[10]

2.2.2 Assessment of the Data Protection Authority

To determine whether the data processed through the Tool constitutes personal data, IMY shall consider 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 of this is negligible.[11]

IMY considers that the data processed constitutes personal data for the following

reasons. The investigation shows that CDON has implemented the Tool by

inserting a
JavaScript code (a tag), as specified by Google, in the source code of the Website. While
When the page is loaded in the visitor's browser, the JavaScript code is loaded from Google LLC's servers and executed locally in the visitor's browser. At the same time, a cookie is placed in the visitor's browser and saved on the computer. The cookie contains a text file that collects information about the visitor's behaviour on the Website. Among other things, a unique identifier is determined 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 transferred via the JavaScript code from the complainant's browser to Google LLC's servers:

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

During the complainant's visit (as referred to in paragraph 1 above), those identifiers were placed in cookies called '_gads', '_ga' and '_gid' and subsequently transmitted to Google LLC. Those identifiers were created for the purpose of distinguishing individual visitors, such as the complainant. The unique identifiers thus make visitors to the Website identifiable. Even if such unique identifiers (as referred to in paragraph 1 above) would not in themselves be considered to make individuals identifiable, it must nevertheless be taken into account that in the present case those unique identifiers can be combined with additional elements (as referred to in paragraphs 2 to 4 above) and that it is possible to draw conclusions in relation to information (as referred to in paragraphs 2 to 4 above) that result in data constituting personal data, notwithstanding the fact that the IP address is not transmitted in its entirety.

[9] ECJ judgment Breyer, C-582/14, EU:C:2016:779, paragraphs 45-46.
[10] Judgment of the Court of Justice of the European Union, M.I.C.M, C-597/19, EU:C:2021:492, paragraphs 102-104 and

judgment Breyer, C-582/14, EU:C:2016:779, paragraph 49.

[11] See Kammarrätten i Göteborgs judgment of 11 November 2021 in case no. 2232-21, agreeing with the lower court's assessment.

The combination of data (according to points 1-4 above) means that individual visitors to the Website become even more distinguishable. It is thus 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 distinguishing (through the word "screening" in recital 26 of the GDPR, "singling out" in the English version) is in itself sufficient to make the visitor indirectly identifiable. It is also not required that Google or CDON intend 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 someone else are *any means that can reasonably* be used for the purpose of identifying the complainant. Examples of *objective means that can reasonably be used* include the availability of additional information from a third party that would enable the complainant to be identified, taking into account both the technology available at the time of identification and the cost (time) of identification.

IMY notes that the CJEU, in the M.I.C.M. and Breyer judgements, has established that dynamic IP addresses constitute personal data in relation to the person processing them, where that person also has a lawful possibility of identifying the holders of the internet connections by means of the additional information available to third parties.[12] IP addresses do not lose their character as personal data simply because the means of identification are held by third parties. The Breyer and M.I.C.M. judgements should be interpreted on the basis of what is actually stated in the judgements, i.e. that if there is a legal possibility to access additional information for the purpose of identifying the complainant, it is objectively clear that there is a "*means reasonably likely to be used*" to identify the complainant. According to IMY, the judgements should not be read in a contradictory manner, in the sense that a legal possibility to access data that can link IP addresses to natural persons must be demonstrated in order for the IP addresses to be considered personal data. An interpretation of the concept of personal data that means that it must always be demonstrated that there is a *legal possibility to* link such data to a natural person would, according to IMY, entail a significant limitation of the regulation's scope of protection, and open up opportunities to circumvent the protection in the regulation. This interpretation would, among other things, be contrary to the purpose of the regulation as set out in Article 1(2) of the GDPR. The Breyer judgment was decided under the previously applicable Directive 95/46, and the concept of 'singling out' as set out in recital 26 of the current Regulation (that knowledge of the actual name or physical address of the visitor is not required, as the distinction is in itself sufficient to make the visitor identifiable), was not mentioned in the previously applicable Directive as a method of identifying personal data.

In this context, there are also other data (as described in paragraphs 1 to 3 above) with which the IP address can be combined to enable identification. Google's action of truncating[13] an IP address means that the IP address is still distinguishable, as it can be combined with other data transferred to third countries (to the US). This allows for identification, which in itself is sufficient for the data to collectively constitute personal data.

---

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

[13] IP address truncation 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 itself can only be one of 256 options. The effect of this measure is that the IP address is still distinguishable from the other IP addresses (255 options), as the IP address can be linked to other data transmitted (e.g. device and time of visit) to third countries.

In addition, several other EU/EEA supervisory authorities have decided that a 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 (as described in paragraphs 1 to 3 above), thus allowing for data segregation and IP address identification, 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. According to Article 4(5) of the GDPR, the pseudonymisation of personal data means that the data - like dynamic IP addresses - cannot be directly attributed to a specific data subject without the use of supplementary information. According to recital 26 of the GDPR, such data should be considered as data relating to an identifiable natural person.

A narrower interpretation of the concept of personal data would, according to IMY, undermine the scope of the right to the protection of personal data, guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, as it would allow data controllers to specifically identify individuals together with personal data (e.g. when they visit a certain website) while denying individuals the right to protection against the dissemination of such data about them. Such an interpretation would undermine the level of protection of individuals and would not be compatible with the wide scope of application of data protection rules as recognised by the case law of the Court of Justice of the European Union.[15]

Furthermore, because the complainant was logged in to his Google account when visiting the Website, CDON has processed data from which conclusions could be drawn about the individual based on his or her registration with Google. According to Google's statement, the implementation of the Tool on a website makes it possible to obtain information that a user of a Google account (i.e. a registrant) has visited the website in question. Admittedly, Google states that certain conditions must be met for it to receive such information, such as that the user (the complainant) has not deactivated the processing and display of personalised advertisements. Since the complainant was logged in to his Google account when he visited 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 clear from the complaint that no personalised ads were displayed does not mean that Google cannot obtain information about the logged-in user's visit to the Website.

IMY finds that, in light of the unique identifiers that can identify the browser or device, the possibility of identifying the individual through his or her Google account, the dynamic IP addresses and the possibility of combining these with additional data, CDON's use of the Tool on a website involves the processing of personal data.

[14] Austria's supervisory authority (Datenschultzbehörde) decision of 22 April 2022 regarding the Google Analytics complaint represented by NOYB with local case number 1354838270, France's supervisory authority (CNIL) decision of 10 February 2022 represented by NOYB and Italy's supervisory authority (Garante) decision of 9 June 2022 regarding the Google Analytics complaint represented by NOYB, local case number 9782890.
[15] See, for example, CJEU, Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:C:2021:504, paragraph 61; Nowak, C-434/16, EU:C:2017:994, paragraph 33; and Rijkeboer, C-553/07, EU:C:2009:293, paragraph 59.

2.3 CDON is the data controller for the processing

Controller includes a legal person who alone or jointly with others determines the purposes and means of the processing of personal data (Article 4(7) of the GDPR). Processor includes a legal person who processes personal data on behalf of the controller (Article 4(8) of the GDPR).

The answers provided by CDON show that CDON has made the decision to implement the Tool on the Website. Furthermore, it appears that CDON's purpose in doing so 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, by deciding to implement the Tool on the Website for that purpose, CDON has determined the purposes and means of the collection and subsequent transfer of those 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.

According to Article 44 of the GDPR, entitled 'General principle of data transfer', inter alia, the transfer of personal data undergoing processing or intended for processing after transfer to a third country - i.e. a country outside the EU/EEA - may only take place provided that the controller and processor, subject to the other provisions of the GDPR, comply with the conditions set out in Chapter V. All the provisions of that chapter are to be applied in order to ensure that the level of protection of natural persons ensured by the GDPR is not undermined.

Chapter V of the GDPR provides tools that can be used for transfers to third countries to ensure a level of protection essentially equivalent to that guaranteed in the EU/EEA. These include transfers under an adequacy decision (Article 45) and transfers subject to appropriate safeguards (Article 46). There are also exceptions for specific situations (Article 49).

In Schrems II, the CJEU annulled the previous adequacy decision for the US.[16] In the absence of an adequacy decision since July 2020, transfers to the US cannot be based on Article 45.

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

[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 in the European Union and the United States and the judgment of the Court of Justice of the European Union in Facebook Ireland and Schrems (Schrems II), C- 311/18, EU:C:2020:559.

conditions that statutory rights of data subjects and effective legal remedies for data subjects are available. 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 CJEU did not reject standard contractual clauses as a transfer tool. However, the Court noted that they are not binding on the authorities of the third country. In that regard, the CJEU stated that "[a]*lthough there are thus situations in which, depending on the legal situation and the practice in force in the third country concerned, the recipient of such a transfer may be able to guarantee the necessary protection of data solely on the basis of the standard data protection clauses, there are other situations in which the provisions of those clauses cannot be a sufficient means of ensuring in practice effective protection of the personal data transferred to the third country concerned."* According to the CJEU, that is *"in particular the case where the legislation of that third country authorises the authorities of that third country to interfere with the rights of the data subjects in respect of those data."*[17]

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

> 'It therefore follows that the standard data protection clauses adopted by the Commission on the basis of point (c) of Article 46(2) of that regulation are intended solely to provide controllers or their processors established in the Union with contractual safeguards which are applied uniformly in all third countries and thus independently of the level of protection ensured in each of those countries. Since those standardised data protection clauses, by their nature, cannot result in safeguards that go beyond a contractual obligation to ensure compliance with the level of protection required by Union law, it may be necessary, depending on the situation in a particular third country, for the controller to take additional measures to ensure compliance with the level of protection".*[18]*

The recommendations of the European Data Protection Board (EDPB) on the implications of the judgement[19] clarify that if the assessment of the law and practice of the third country means that the protection that the transfer tool is supposed to ensure cannot be maintained in practice, the exporter must, as a rule, either suspend the transfer or take appropriate additional safeguards. In this regard, the EDPB notes that "*additional measures can only be considered effective within the meaning of the ECJ's Schrems II judgment if and to the extent that they address - alone or in combination - the specific deficiencies identified in the assessment of the situation in the third country with regard to its laws and practices applicable to the transfer"*.[20]

---

[17] points 125-126.
[18] point 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, paragraph 75; IMY translation.

The EDPB recommendations indicate that such additional safeguards can be divided into three categories: contractual, organisational and technical.[21]

With regard to *contractual* measures, the EDPB states that such measures "*[...] can complement and reinforce the safeguards provided by the transfer tool and relevant legislation in the third country [...] Given the nature of contractual measures, which generally cannot bind the authorities of that third country as they are not parties to the agreement, these measures may often need to be combined with other technical and organisational measures to provide the required level of data protection [...]".*[22]

With regard to *organisational measures, the* EDPB stresses that "*[s]electing and implementing one or more of these measures will not necessarily and systematically ensure that [a] transfer meets the basic equivalence standard required by EU law. Depending on the specific circumstances of the transfer and the assessment of the third country's legislation, organisational measures are required to complement contractual and/or technical measures to ensure a level of protection of personal data that is substantially equivalent to that guaranteed in the EU/EEA*".[23]

With regard to *technical* measures, the EDPB points out that "*these measures will be necessary in particular when the legislation of that country imposes obligations on the importer which are contrary to the guarantees of Article 46 of the GDPR transfer tool and which may, in particular, infringe the contractual guarantee of substantially equivalent protection against access by the authorities of that third country*".[24] In this regard, *the* EDPB states that *"the measures set out [in the Recommendations] are intended to ensure that access to the transferred data by public authorities in third countries does not jeopardise the effectiveness of the appropriate safeguards in Article 46 of the GDPR transfer tool. These measures would be necessary to ensure an essentially equivalent level of protection to that guaranteed in the EU/EEA, even if the access by public authorities is in accordance with the law of the importer's country, where such access in practice goes beyond what is necessary and proportionate in a democratic society. The purpose of these measures is to prevent potentially unauthorised access by preventing the authorities from identifying the data subjects, drawing conclusions about them, identifying them in another context or linking the transferred data to other data sets that may include, inter alia, network identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts*".[25]

2.4.2 Assessment of the Data Protection Authority

2.4.2.1 Applicable transfer tool

The investigation shows that CDON and Google have entered into standardised data protection provisions (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, paragraph 52.
[22] EDPB Recommendations 01/2020, paragraph 99; IMY translation.
[23] EDPB Recommendations 01/2020, paragraph 128; IMY translation.
[24] EDPB Recommendations 01/2020, paragraph 77; IMY translation.
[25] EDPB Recommendations 01/2020, paragraph 79; IMY translation.

2.4.2.2 Legislation and situation in the third country
As stated in the Schrems II judgement, the use of standard contractual clauses may require additional safeguards to complement them. Therefore, an analysis of the legislation of the third country in question needs to be carried out.

IMY considers that the analysis already made by the CJEU in Schrems II, which relates to similar circumstances, is relevant and up-to-date, and can thus be used as a basis for the assessment in this case without any further analysis of the US legal situation.

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

In Schrems II, the CJEU held that the US surveillance programmes based on 702 FISA, Executive Order 12333 ('E.O. 12333') and Presidential Policy Directive 28 ('PPD-28') of the US legislation do not meet the minimum requirements of EU law under 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. Moreover, the Court found that the surveillance programmes do not provide data subjects with rights that can be enforced against the US authorities in court, which means that those persons are not entitled 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 personal data transferred.

2.4.2.3 Additional protection measures implemented by Google and CDON
The next question is whether CDON has taken sufficient additional safeguards.

As data controller and exporter of the personal data, CDON is obliged to ensure compliance with the rules of the General Data Protection Regulation. This responsibility includes, among other things, assessing in each individual case, when transferring personal data to third countries, which additional protection measures should be used and to what extent, including evaluating whether the measures taken by the recipient (Google) and the exporter (CDON) together are sufficient to achieve an acceptable level of protection.

2.4.2.3.1 Google's additional safeguards
Google LLC, as an importer of personal data, has taken contractual, organisational and technical measures to supplement the standard contractual clauses. In its statement of 9 April 2021, Google described the measures it has taken.

The question is whether the additional safeguards adopted by CDON and Google LLC are effective, in other words, prevent the possibility for US intelligence services to access the transferred personal data.

With regard to the *legal and organisational measures*, it can be noted that neither the information to users of the Tool (such as CDON),[27] the publication of a

[26] Paragraphs 184 and 192; paragraph 259 et seq.
[27] Regardless of whether such notification would even be permitted under US law.

transparency report or a publicly available '*government request handling policy*' prevents or reduces the ability of US intelligence agencies *to* access the personal data. Furthermore, it is not described what it means that Google LLC's conducts a "*thorough review of each request*" for "lawfulness" from US intelligence agencies. IMY notes that this does not affect the lawfulness 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, it can be noted that neither Google LLC nor CDON has clarified how the measures described - such as protection of communications between Google services, protection of data during transfer between data centres, protection of communications between users and websites or 'physical security' - prevent or reduce the ability of US intelligence agencies to access the data on the basis of the US regulatory framework.

However, with regard to the encryption technology used - for example, for 'data at rest' in data centres, which Google LLC mentions as a technical measure - Google LLC, as an importer of personal data, still has an obligation to grant access to or transfer imported personal data held by Google LLC, including any encryption keys required to make the data intelligible.[28] Thus, such a technical measure cannot be considered effective as long as Google LLC is able to access the personal data in plaintext.

As regards Google LLC's statement that *"to the extent that Google Analytics measurement information transmitted by website owners constitutes personal data, it may be considered to be pseudonymised*", it can be noted 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 technique, but the unique identifiers, as described above, have the specific purpose of distinguishing users and not to serve as protection. In addition, the possibility to combine unique identifiers with other data (e.g. metadata from browsers or devices and the IP address) and the possibility to link such information to a Google account for logged-in users, as described above, makes individuals identifiable.

With regard to Google's "anonymisation of IP addresses" measure in the form of truncation[29], it is not clear from Google's response whether this measure takes place before the transfer, or whether the entire IP address is transferred to the US and truncated only after the transfer to the US. Thus, from a technical point of view, it has not been demonstrated that there is no potential access to the entire IP address before the last octet is truncated.

Against this background, IMY concludes that the additional safeguards adopted by Google are not effective, as they do not prevent the possibility for US intelligence agencies to access the personal data or render such access ineffective.

2.4.2.3.2 CDON's own additional protection measures

CDON has stated that the company has taken further protective measures in addition to the measures taken by Google. According to CDON, these consist of the activation of

[28] See EDPB Recommendations 01/2020, paragraph 81.
[29] IP address truncation means that asterisks or zeros replace other digits in last octets (last digits of an IP address, a number between 0 and 255).

the function of truncating[30] the last octet of the IP address before transmitting the data to Google, which masks the last octet.[31]

As stated above regarding Google's actions, it is not clear from Google's response whether this action takes place before the transfer or whether the entire IP address is transferred to the United States and truncated only after the transfer to the United States. Thus, from a technical point of view, it has not been shown that after the transfer 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 transmission, it is not a sufficient measure, as the truncated IP address can be linked to other data, as noted by IMY in section 2.2.2 above. in the range 0-255) and because the truncated IP address is distinguishable from other IP addresses, this data can be linked to the other data (as described above in section 2.2.2) and allow for identification, which in itself is sufficient to determine whether the data together is personal data. Even if the masking of the last octet constitutes a privacy enhancing measure, as it limits the scope of data that can be accessed by authorities (in third countries), IMY notes that it is still possible to link the transferred data to other data also transferred to Google LLC (in third countries).

Against this background, IMY concludes that the additional measures taken by CDON in addition to the additional measures taken by Google are not sufficiently effective to prevent the possibility for US intelligence agencies to access the personal data or render such access ineffective.

2.4.2.3.3 Conclusion of the European Data Protection Authority

IMY finds that CDON's and Google's measures are neither individually nor collectively sufficiently effective to prevent US intelligence agencies from accessing the personal data or render such access ineffective.

Against this background, IMY finds that neither standard contractual clauses nor the other measures invoked 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 of data subjects guaranteed by Article 44 of the GDPR.

IMY therefore finds that CDON AB is in breach of Article 44 of the GDPR.

3 Choice of intervention

3.1 Legal regulation

IMY has a number of remedial powers available to it in case of breaches of the GDPR under Article 58(2)(a) to (j) of the GDPR, including reprimand, injunction and penalties.

[30] IP address truncation means that asterisks or zeros replace other digits in last octets (last digits of an IP address, a number between 0 and 255).
[31] See above in the section on what CDON has argued, under the heading "Additional safeguards taken".

IMY shall impose penalty payments in addition to or instead 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 in each case 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 should be imposed, but also in determining the amount of the fine. As stated in recital 148, in the case of a minor infringement, the IMY may, instead of imposing a fine, issue a reprimand under Article 58(2)(b) of the Regulation. The assessment will take into account the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and relevant previous 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 a penalty be imposed?

IMY has above found that the transfers of personal data to the United States that take place via the Google Analytics tool and for which CDON is responsible are contrary to Article 44 of the GDPR. Infringements of that provision can lead to penalties under Article 83.

Given, inter alia, that CDON has transferred a large amount of personal data, that the processing has been ongoing for a long time and that the transfer has meant that the personal data could not be guaranteed the level of protection provided in the EU/EEA, this is not a minor infringement. CDON should therefore be subject to an administrative fine for the identified infringement. See also below under 3.3 for a detailed description of the seriousness of the infringement.

3.2.1 What is the amount of the penalty?

When determining the maximum amount of a fine to be imposed on an undertaking, the definition of an 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) should be used. It follows from the Court's case-law that this includes any entity engaged in an economic activity, regardless of its legal form and the way in which it is financed, and even if the entity is legally composed of several natural or legal persons.[33]

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

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.

---

[32] EDPB Guidelines 8/2020 Guidelines 04/2022 on the calculation of administrative fines under the GDPR (adopted for public consultation on 12 May 2022).
[33] See Judgment in Akzo Nobel, C-516/15, EU:C:2017:314, paragraph 48.

had a turnover of approximately SEK 461 000 000 in that financial year. That amount is less than EUR 20 million and therefore the penalty can be set at an amount of up to EUR 20 million.

In determining the amount of the penalty payment, IMY shall take into account the seriousness of the infringement and shall take into account both aggravating and mitigating circumstances to determine an administrative penalty that is effective, proportionate and dissuasive in the individual case.

IMY considers the following factors to be important in assessing the seriousness of the infringement.

As regards the assessment of the gravity of the infringement, there are initially factors that justify a more serious view of the infringement. CDON has transferred a large amount of personal data to third countries. The transfer has meant that the personal data could not be guaranteed the level of protection provided in the EU/EEA, which in itself is a serious infringement. 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 they have been systematic. IMY also considers that approximately 3 years have now passed since the Court of Justice of the European Union, in its judgment of 16 July 2020, overturned the Commission's decision on the adequacy of protection in the United States[34], thereby changing the conditions for transfers of personal data to the United States.

In the meantime, the EDPB has issued recommendations on the consequences of the judgment, which were put out for public consultation on 10 November 2020 and adopted in final form on 18 June 2021. In addition, several other EU/ESS supervisory authorities have issued orders to cease the use of the Tool until sufficiently effective security measures have been taken by the controllers. These decisions have included cases where controllers have also taken measures such as "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 companies in the US, CDON has not taken its own additional protective measures. Google's measure regarding truncation[36] of IP address means that it is still possible to distinguish the IP address, as it can be linked to other data transferred to third countries (to the US). This enables identification, which means that the data together constitute personal data.

In addition, CDON's website is a popular e-commerce portal offering goods from many different suppliers and is available in several countries and languages. It involves data on a large number of data subjects in the EU/EEA who can be identified indirectly and

---

[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] The Austrian supervisory authority (Datenschultzbehörde) decision of 22 April 2022 regarding the Google Analytics complaint 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 regarding the Google Analytics complaint represented by NOYB, local case number 9782890.
[36] IP address truncation "IP address anonymisation" 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 itself can only be one of 256 options. The effect of this measure is that the IP address can still be distinguished from the other IP addresses (255 options), as the IP address can be linked to other data transmitted (e.g. device and time of visit) to third countries (to the US).

whose data can be linked to other data about them. With regard to the nature of the data, it already follows from CDON's own purpose of the processing - i.e. to be able to draw conclusions about how the data subjects navigate and find their way to the Website - that the data as a whole makes it possible to draw relatively precise conclusions about the privacy of the data subjects and map them, such as what they buy and what goods they are interested in over time. CDON's analysis of the Tool shows that there are proposals for a solution other than the Tool, but the company has chosen not to introduce this solution on the grounds that such a change would be particularly burdensome for the company. CDON's processing of personal data entails risks of serious violation of the rights and freedoms of individuals, which gives CDON a special responsibility that entails high requirements for transfers to third countries, where IMY's overall assessment is that CDON has not demonstrated that the company has made a sufficient analysis and mapping and has not taken the necessary security measures to limit the risks for the data subjects.

At the same time, IMY recognises that there are factors that point in the opposite direction. IMY takes into account the specific situation following the judgment and the interpretation of the EDPB's recommendations, where there was a gap after the transfer tool to the US was rejected by the CJEU in the Commission's previous decision. IMY also takes into account that CDON took some, albeit insufficient, measures to limit the personal data transferred by activating "anonymisation of IP addresses" through truncation.[37] This fact is also taken into account when assessing the gravity of the infringements.

Overall, IMY assesses, in light of the circumstances presented, that the infringements in question are of low severity. The starting point for the calculation of the penalty fee should therefore be set low in relation to the current maximum amount.
In order to ensure a proportionate penalty fee in the individual case, there is also reason to further adjust the starting point for the further calculation downwards already at this stage, taking into account the turnover on which the calculation of the penalty fee is based.

In addition to the assessment of the seriousness of the infringement, IMY must assess whether there are any aggravating or mitigating circumstances that are significant for the size of the administrative fine. IMY assesses that there are no further aggravating or mitigating circumstances, in addition to those considered in the assessment of the severity, that affect the size of the administrative fine.

Based on an overall assessment of the aforementioned circumstances and in light of the fact that the administrative penalty must be effective, proportionate and dissuasive, IMY assesses that the penalty can remain at SEK 300,000 (three hundred thousand).

3.3 Other interventions

In the light of the observed infringement, IMY makes the assessment that CDON should be ordered under Article 58(2)(d) of the General Data Protection Regulation 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 other provisions of Chapter V. This shall be done in particular by ceasing to use the version of the tool.

---

[37] Austria's supervisory authority (Datenschultzbehörde) decision of 22 April 2022 regarding the complaint Google Analytics represented by NOYB with local case number 1354838270, France's supervisory authority (CNIL) decision of 10 February 2022 represented by NOYB and Italy's supervisory authority (Garante) decision of 9 June 2022 regarding the complaint Google Analytics represented by NOYB, local case number 9782890.

Google Analytics used on 14 August 2020, unless adequate safeguards are in place. These measures must be implemented no later than one month after this decision becomes final.

This decision was taken by Director-General Lena Lindgren Schelin after being presented by legal adviser Sandra Arvidsson. David Törngren, Head of Legal Affairs, Catharina Fernquist, Head of Unit and Mats Juhlén, IT and information security specialist, also participated in the final processing.

Lena Lindgren Schelin, 2023-06-30 (This is an electronic signature)

Annex
Annex 1 - Information on the payment of penalties

4 Appeal reference

4.1 How to appeal

If you want to appeal the decision, you should write to the Authority. State in your letter which decision you are appealing and the change you are requesting. The appeal must be received by the Authority no later than three weeks from the date you received the decision. If the appeal has been received in time, the Authority will forward it to the Administrative Court in Stockholm for review.

You can email the appeal to the Swedish Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or data that may be subject to confidentiality. The Authority's contact details can be found on the first page of the decision.