Integritetsskydds myndigheten

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision in case with national reference number, DI-2020-11370. Only the Swedish version of the decision is deemed authentic

Registration number:
DI-2020-11370

Date of decision:
2023-06-30

Final decision under the General Data Protection Regulation – Dagens Industri AB´s 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 Authority for Privacy Protection finds that the investigation has shown that Dagens Industri Aktiebolag processes personal data in breach of Article 44 of the GDPR[1] by using the Google Analytics tool provided by Google LLC on its website www.di.se, and thereby transferring personal data to third countries without the conditions laid down in Chapter V of the Regulation being met, since 14 August 2020 and until the date of this decision.

Pursuant to Article 58(2)(d) of the GDPR, the Dagens Industri Aktiebolag 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. In particular, Dagens Industri Aktiebolag shall cease to use the version of the Google Analytics tool used on 14 August 2020, unless appropriate safeguards have been taken. The measures shall be implemented no later than one month after the date of entry into force of this Decision.

1 Presentation on the supervisory report

1.1 Processing

The Swedish Integrity Authority for Protection Authority (IMY) has initiated supervision regarding Dagens Industri AB (hereinafter Dagens Industri 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.di.se (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 GDPR. The supervisory authorities concerned has been the data protection authorities in Germany, Norway, Denmark, Estonia and Portugal.

1.2 What is stated in the complaint

The complainant essentially stated 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 Dagens Industri's 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. Dagens Industri) and is therefore to be classified as the company's data processor.

During the visit to the company's website, Dagens Industri 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, Dagens Industri 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), the company[2] could no longer rely on an adequacy decision under Article 45 of the GDPR for the transfer of data to the United States. Dagens Industri 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 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. Dagens Industri cannot therefore ensure adequate protection of the complainant's personal data when it is transmitted to Google.

1.3 What Dagens Industri has stated

Dagens Industri Aktiebolag has 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 Dagens Industri, 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.

---

[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.

The purpose of embedding the code for the Tool on the Website is to enable Dagens Industri to analyse how the Website is used, in particular to be able to monitor the use of the Website over time.

The Website is aimed at Swedish visitors, but it cannot be excluded that individuals from other countries have visited the Website and thus may be included in the statistics.

The data (including any personal data) transmitted to the Tool may be stored on servers in different countries, including the United States. As a user of the Tool, it is not possible to control which servers are used to store data in the Tool.

1.3.2 Recipients of the data
In the context of Dagens Industri's use of the Tool on the Website, personal data is disclosed to a number of actors, all of which are data processors or sub-processors to Dagens Industri, including Google LLC, Google Ireland Ltd and their sub-processors.

1.3.3 The data processed in the Tool and what constitutes personal data
Within the framework of Dagens Industri's use of the Tool on the Website, the company and its personal data processors (the recipients) process the following data.

- *Page* view data — such as URL, clicks in menus, articles visited, reading time, and how long the visitor is watching a video.
- *Device technical information* — such as cookie value (which is hashed before it is transferred to the Tool, but was not hashed when the complainant visited the Website), operating system and screen size.
- *User category* — for example, a flag that shows whether the visitor is a subscriber or not.[4]
- *So-called "own dimensions"* — for example, which version of the publishing platform on which a page view took place, information about article (e.g. author).
- *IP Addresses* — The IP address is processed both when Google Analytics *is measured script and when* measured data are to be *transferred* to the Tool. The IP address processed together with measured data (page view data, etc.) is anonymised through the company's proprietary process and which is handled on an EU-based infrastructure before it is sent together with the measured data to the Tool (see more about this below).

Dagens Industri considers that the *categories* page view data, technical information about device, user category and "own dimensions" can be considered personal data only in cases where the company can link this data to an individual through additional information that the company has in other systems, which is not always the case. Dagens Industri considers IP addresses as personal data until these are anonymised.

1.3.4 Categories of persons concerned by the treatment
The *categories* of persons concerned by the processing are visitors to the Website. It can be Dagens Industri's paying subscribers or visitors without a digital account.

[4] Please note that identifying information such as actual subscription ID is not transferred, but only a value representing the category "subscriber" or "not subscriber" (1 or 0).

Data on particularly vulnerable persons are not processed. The Website is primarily aimed at adults in their professional role or who have an interest in economics and nutrition issues. It is not aimed at children or other particularly vulnerable groups.

1.3.5 When the code for the Tool is executed and recipients are accessed
The code for the content of the Tool, i.e. the script that measures the data sent to the Tool, is only executed if the visitor has given their consent to Dagens Industri using analytics cookies on the Website. If the visitor has given their consent, the data measured by the script will first be sent to Dagens Industri's proxy server, where several security-enhancing measures are implemented, such as anonymisation of IP address. A subset of the measured data is then transferred encrypted from the proxy server to the tool provided by Google (see below).

Google LLC, Google Ireland and other data processors and subprocessors have access to the pseudonymised data stored in the Tool to the extent necessary for the processor or subprocessor to perform the service, including support and troubleshooting services.

1.3.6 How long the personal data are stored
The data measured on the Website and transmitted to the Tool will be stored in the Tool for 26 months and then deleted. Dagens Industri´s saves the data in order to analyse the use of the Website over time, in order to be able to make annual comparisons and thereby analyse how the usage changes. Dagens Industri has considered that it is necessary to at least be able to compare the use over two years cycles. In order to analyse and produce statistics on these changes, the company needs to save the measured data for 26 months.

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

1.3.8 Dagens Industri´s relationship with Google LLC
The Tool is provided by agreement between Dagens Industri and a Swedish limited company (hereinafter the "Supplier"). Google Ireland Ltd is in turn a subcontractor to the supplier. Dagens Industri has entered into a personal data processor agreement with the supplier, which regulates the supplier's and its sub-processe´s personal data processing.

Since the purposes and means of the processing as a whole are determined by Dagens Industri, Google LLC and Google Ireland Ltd are processors for the personal data processing that becomes relevant in relation to the Tool.

Dagens Industri has also entered into a data processing agreement directly with Google LLC to comply with the formal requirements of the standard contractual clauses, i.e. that these be formally entered into directly between the controller and the third country processor.

1.3.9 Ensure that processing is not carried out for the purposes of the recipients

1.3.9.1 Generally
Dagens Industri cares to use only suppliers that can meet the company's high requirements for safe and lawful personal data processing. Before selecting a particular supplier, an assessment is made of the supplier's ability to maintain an acceptable level of security, including protecting personal data to be processed.

Dagens Industri has also developed an audit plan in which the company intends to carry out audits of the most important suppliers, based on a rolling schedule. Dagens Industri has also engages in a continuous dialogue with Google, where security and data protection issues are discussed.

1.3.9.2 Contracts with the Supplier

Through the assistant agreement with the supplier and the documented instructions given by Dagens Industri in this respect, it has been contractually ensured that the supplier and its sub-processors do not process personal data for their own or third parties' purposes. The Assistance Agreement thus contains special provisions (section 3.2.1) that the supplier may only process personal data in accordance with Dagens Industri's documented instructions. Annex 2 to the Processing Agreement clarifies that the supplier under no circumstances has the right to process personal data for his own purposes.

As an incentive to comply with the requirements set out in the assistance agreement and to point out its weight, the Supplier has a liability to Dagens Industri if the Supplier should violate the agreement or applicable data protection legislation and this causes damage to Dagens Industri.

The assistance agreement with the supplier also enables Dagens Industri to request documentation and carry out audits of systems and procedures to ensure that the processing is carried out in accordance with Dagens Industri's documented instructions and applicable data protection legislation.

If Dagens Industri has reason to believe that the supplier does not comply with the requirements set out in the assistance agreement, Dagens Industri intends to conduct such an audit. The Provider also has the right to request documentation and to conduct audits in relation to Google (Section 7.5 of Google's Agreement).

Dagens Industri may also request to conduct audits of Google's systems and procedures in accordance with the Assistant Agreement with the Supplier (Section 8.5).

1.3.10 Description of Dagens industri´s use of the Tool

Dagens Industri uses the Tool to collect quantitative data, web statistics, how the Website is used, and perform analyses based on this data. For example, web statistics can show which pages are most visited, which route visitors take through the Website, and from which pages visitors leave the Website. Web analytics can also provide insight into the frequency of visits and what content is visited for the longest time. For example, the analysis carried out using the Tool can serve as the basis for product improvements.

1.3.11 Own checks on transfers affected by the judgment in Schrems II

Following the publication of the Schrems II judgment on 16 July 2020, Dagens Industri launched a project to generally map transfers of personal data to third countries at the end of July 2020. The project did not specifically address the tool, but concerned third country transfers in general. In connection with Dagens Industri's becoming aware of, inter alia, the complaint at issue, a project specifically related to the use of the Tool was initiated on 18 August 2020. Relatively immediately after the judgment, the company was able to conclude that it is relevant to the data transmission that takes place within the framework of the Tool and Dagens Industri has subsequently implemented relevant safeguards, see below.

1.3.12 Transfer tools under Chapter V of the GDPR

Dagens Industri has entered into a personal data processing agreement directly with Google LLC. Google's standard contractual clauses are part of the assistance agreement. The assistant agreement states that Google is bound by the clauses (paragraph 10.2). The clauses are based on Commission Decision 2010/87/EU for transfers from a controller within the EU/EEA to a processor outside the EU/EEA. These terms and conditions apply automatically upon the conclusion of Google's Data Processing Agreement and thus do not need to be signed separately in order to be applicable. This is apparent from the preamble to Google's standard contractual clauses. Under Swedish law, which applies to the standard contractual clauses, this means that they become part of the contract.

Google's standard contractual clauses are also part of the Data Processing Agreement with the supplier in accordance with Annex 2 of the Processing Agreement with the supplier.

Dagens Industri has also entered into a data processor agreement with the supplier, in which Google Ireland Ltd acts as subprocessor and which in turn has some sub-processors in third countries. For the purposes of this Agreement, Google's standard contractual clauses are also applied as a transfer tool.

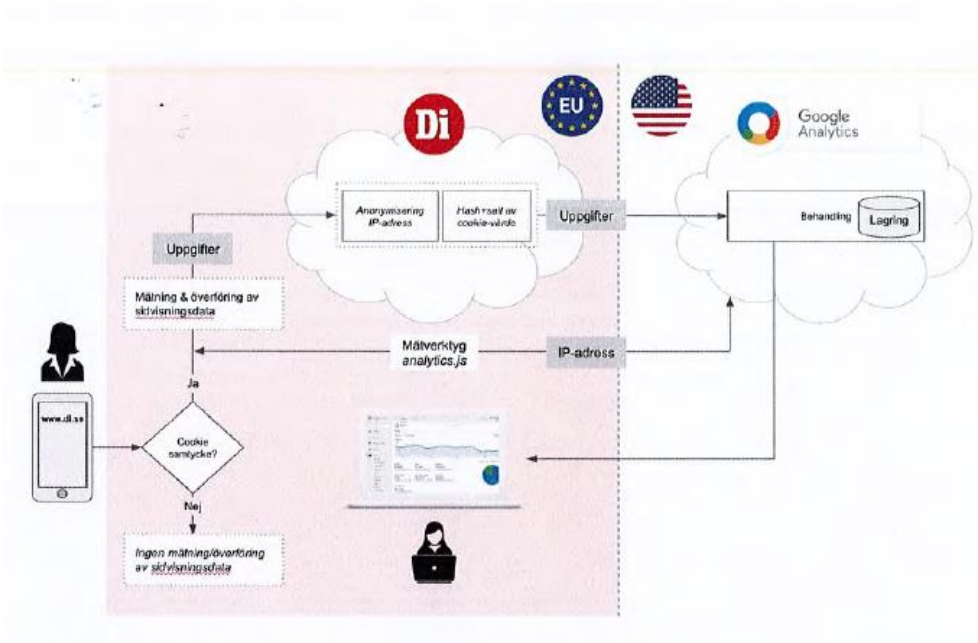
1.3.13 Verification of obstacles to compliance in third country legislation

Dagens Industri has not yet been able to establish with certainty whether there is anything in third country legislation that prohibits beneficiaries from fulfilling their contractual obligations under the standard contractual clauses. The company has therefore presumed that this is the case and has put in place specific technical measures to ensure that the protection of the data processed in the Tool reaches an acceptable level.

1.3.14 Supplementary measures taken in addition to those taken by Google

1.3.14.1 Introduction

Dagens industri has carried out a comprehensive mapping of the life cycle of personal-data processed in the Tool, identifying and implementing a number of supplementary measures. The measures are visualised at a glance in the picture below, and are further commented in the following sections.



1.3.14.2 Control of the collection and transmission of data to the Tool

A common way of using the Tool, unless supplementary measures are taken, means that the data measured through the Website's measuring script is transferred directly to the servers of the Tool, without first going through a control point of the controller using the tool.

Because the Tool's servers may be located inside and outside the EU/EEA, the use of the tool may lead to the transfer of measured data to third countries. The Tool has a function that allows users of the tool to choose to anonymise the IP address (trunking)[5] that is transmitted together with the measured data. Since anonymisation occurs only after the IP address is transferred to Google Analytics servers, according to Dagens Industri, a third country transfer occurs before anonymisation takes place.

Dagens Industri has taken supplementary measures before data is transferred to the Tool. In order to take control of what data is transferred to the servers of the Tool outside the EU/EEA, the Company has implemented technical measures whereby the data collected through Google Analytics measurement script on the Website are transferred in a first step to a proxy server located in the EU where the data are processed in order to avoid that they can be used to identify an individual accordingly. The software used has been developed and owned by Dagens Industri, and is hosted by Google Ireland Ltd as part of the Google Cloud Platform ("GCP"). The GCP is thus used only as leased infrastructure to run the proxy server code on. The data processed on the GCP takes place exclusively at data centres in the EU. Dagens industri is responsible for the personal data that takes place in the proxy server.

By introducing this control point, Dagens Industri can ensure that no data is transferred to servers outside the EU/EEA without having first undergone protective measures (see further below). Transmission to the proxy server is encrypted using Secure Sockets Layer ("SSL"), a technology that is encrypted communication between a web-server and a serve).

[5] 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).

1.3.14.3 Anonymisation of IP address and algorithm

The data that in some cases can be linked to an individual and transferred from the Website to the proxy server is the IP address and cookie value. The examples below illustrate how these numbers can look before and after they are processed on the proxyserver.

Before processing on proxy server:

Data

- IP address: clear text, e.g. 176.10.253.34
- Cookie value: clear text, e.g. 744100309.1604572939

Before transferring the measured data to the Tool, the following is performed on the proxy server:

- *Anonymisation of IP address*. The visitor's IP address is anonymised by generalisation and aggregation where the last octet of the IPv4 address is replaced by ".0".
- *Hashing of the cookie value*. The cookie value measured on the Website can either be completely anonymous (when the company *cannot* link the cookie value to data in its other systems) or constitute a pseudonymised personal data (when the company can link the cookie value to data in its other systems). As a supplementary measure before transferring to the tool, the cookie value from the visitor's client with a "salt" has been collected.[6] The hashing of the cookie value further protects against the risk that U.S. authorities may link "intercepted data" (i.e. data that could possibly be read through signals intelligence programs either "at rest" in the Tool or "in transfer") with identifying data to which U.S. authorities might otherwise be able to access.

If *the* actions described above have been carried out, the IP address and the cookie value may, for example, look as follows:

Data

- IP address: anonymised, e.g. 176.10.253.00
- Cookie value: hashad, e.g. 35009a79-1a05-49d7-b876-2b884d0f825b

The data is then transferred via SSL encryption from the proxy server to the Tool.

Anonymisation of the visitor's IP address takes place when it is to be transmitted together with the measured page view data, etc. (see above for which data points are measured).

Prior to that, the IP address was exposed to the Tool when Google Analytics measured script via encrypted transmission was loaded into the visitor's browser from the Tool's server. It is not possible to link the IP address to the page view data etc. which is later measured on the Website. Dagens Industri has therefore assessed that

[6] Cf. information on "Keyed-hash function with stored key" in the Article 29 Working Party's guidance on anonymisation techniques.

this exposure to the IP address does not pose a risk of privacy for visitors to the Website.

Google LLC may indirectly derive the time of the visit, but this possibility is very limited. Google has configured the server whereupon 'analytics.js' is provided in such a way that the JavaScript file is cached in the application cache of the receiving terminal for two hours, regardless of which website it is first obtained through (i.e. not necessarily on the Website). During this time period, no further calls are made in which the IP address is exposed in its entirety, which means that the measured page view data transmitted via Dagens Industri's proxy server to Google LLC (first transmission) very rarely have a corresponding time equivalent machine log of Google LLC linked to the transmission via "analytics.js" (second transmission). In combination with the fact that visitors most often use the Website as a source of information in the work and/or during the previous two hours visited another website that uses Google Analytics (maximum likely given that about 74 % of the world's 10,000 most popular websites present) a large percentage of visits to the Website only result in transmitted page view data from Dagens Industri's proxy server and no loading of the Tool and associated transmission of IP address. This greatly complicates any attempt to link machine logs from the transfer of the Tool and transmitted page view data from Dagens Industri's proxy server and reduces according to Dagens Industri risk to beyond "reasonable probability".

1.3.14.4 More on checking that further measures can be implemented in practice, etc.
Dagens Industri considerations regarding the measures implemented by the company are based on the EDPB's recommendations on how individual third country transfers should be assessed according to their specific legal context (paragraph 33).[7]

The security-enhancing measures consist primarily of the responsibility and control that Dagens Industri has taken over the phases of the life cycle before transferring the data to the Tool. The risk assessment has had as a starting point that the data subject's protection is best achieved by the fact that the data transferred outside the EU/EEA are disconnected from the data subject and his/her technical unit used to visit the Website, and that the Company controls the process that ensures that these actions are carried out.

1.3.14.5 Dagens Industri´s conclusion on an adequate level of safety protection
Taking into account the measures implemented, Dagens Industri considers that the risk that the data subjects' privacy or rights would be violated by the use of the Tool is very small. The company's overall assessment is therefore that an adequate level of protection is achieved through the supplementary measures implemented.

1.3.15 Dagens industri´s assessment and conclusion regarding whether the data can be considered identifiable

1.3.15.1 The Company's assessment of whether the data can be considered identifiable
Dagens Industri believes that it is not self-evident that an assessment leads to the data in question — IP address, certain system information and visited URL — constitute personal data.

[7] EDPB Recommendation 01/2020 on measures to complement transfer tools to ensure compliance with the EU level of personal data protection Version 2.0 Adopted on 18 June 2021

Recital 26 of the GDPR states, inter alia:

'*In order to determine whether a natural person is identifiable, account should be taken of all means, such as excavation, which, either by the controller or by another person, may reasonably be used to identify the natural person directly or indirectly. In order to determine whether means are reasonably likely to identify the natural person, account should be taken of all objective factors, such as the costs and time needed for identification, taking into account the technology available at the time of processing as technological progress*.'

In its guidance on the concept of personal data,[8] the Article 29 Working Party has further clarified how the assessment should be carried out:

Recital 26 to Directive 95/46[9] (repealed) *pays particular attention to the term "iidentifiable"* " when it reads that "whereas to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." This means that a mere hypothetical possibility to single out the individual is not enough to consider the person as "identifiable". If, taking into account "all the means likely reasonably to be used by the controller or any other person", that possibility does not exist or is negligible, the person should not be considered as "identifiable", and the information would not be considered as "personal data". The criterion of "all the means likely reasonably to be used either by the controller or by any other person" should in particular take into account all the factors at stake. The cost of conducting identification is one factor, but not the only one. The intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risk of organisational dysfunctions (e.g. breaches of confidentiality duties) and technical failures should all be taken into account.*"*[10]

In addition, the guidance states:

"One relevant factor, as mentioned before, for assessing "all the means likely reasonably to be used" to identify the persons will in fact be the purpose pursued by the data controller in the data processing."[11]

1.3.15.2 Dagens Industri´s conclusion as to whether the data can be considered identifiable

Dagens Industri has concluded that in order for it to be personal data according to the GDPR, the assessment of whether individuals are identifiable should be based on all relevant circumstances and assess the reasonable likelihood of identification, of which the purpose of the processing is a circumstance. Since the purpose of the processing is not to identify individuals, technical protection measures are an extra important factor in assessing whether individuals may be identified.

Against this background, Dagens Industri concludes that it is not self-evident that an assessment in accordance with the Article 29 Working Party's guidance means that the data in question — IP address, certain system information and web address visited

[8] WP 136. Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, adopted on 20 June 2007
[9] Directive 95/46/EC of theEuropean Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[10] WP 136. Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, adopted on 20 June 2007, page 15.
[11] WP 136. Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, adopted on 20 June 2007, pages 16 and 17.

— constitute personal data.

The assessment that individuals are not identifiable has been made taking into account the circumstances shown in i.e. (i) the cost of identification, (ii) the purpose of the processing, (iii) the structure of the processing, (iv) the benefits that the controller expects from the processing, (v) the interests at stake for the natural person, and (vi) the duration of the processing. The purpose of the processing is not to identify individuals but constitute technical protection measures. According to Dagens Industri, it is not at all obvious that an assessment in accordance with the guidance leads to the data in question — IP address, certain system information and visited URL — constitute personal data.

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. Dagens Industri 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 optimize 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 (UUID) identification 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.

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 Dagens Industri transfers personal data to the third country USA within the framework of the Tool and whether the company has legal support for it in Chapter V of the GDPR. Supervision does not apply if the Dagens Industri's personal data processing is otherwise in accordance with the GDPR.

2.2 This is the processing of personal data

2.2.1 Applicable provisions, etc.

In order to determine whether the data processed through the Tool constitute personal data, IMY shall decide whether Google or Dagens Industri, through the implementation of the Tool, can identify individuals, e.g. the complainant, when visiting the Website or whether the risk is negligible.[12]

[12] 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.

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

The investigation shows that Dagens Industri 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's 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 Dagens Industri (i.e. the Dagens Industri 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 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 addresses 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 Dagens Industri 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.[13] 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[14] the truncation of an IP address means that the IP address can still be 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.[15]

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.

---

[13] 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.
[14] 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), 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 the IP address can be linked with other transmitted data (e.g. information on the entity and time of visit) to third countries.
[15] 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.

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.[16]

Furthermore, Dagens Industri, 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, Dagens Industri's use of the Tool on a website, means the processing of personal data.

2.3 Dagens Industri 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 Dagens Industri indicate that the company has made the decision to implement the Tool on the Website. It also appears that Dagens Industri'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 Dagens Industri, 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. Dagens Industri is therefore the data controller for this processing.

[16] 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.

2.4 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 whether Dagens Industri's transfer of personal data to the United States complies 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.[17] In the absence of an adequacy decision since July 2020, cannot transfers to the United States 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 only transfer personal data to a third country after having taken appropriate safeguards, and subject to the 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.*'[18]

---

[17] 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.
[18] Points 125-126.

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'.[19]

The recommendations of the European Data Protection Board (EDPB) on the consequences of the judgment[20] 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*.'[21]

The recommendations of the EDPB show that such supplementary measures can be divided into three categories: contractual, organisational and technical.[22]

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 [...]'.*[23]

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*

---

[19] Paragraph 133.
[20] 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").
[21] EDPB Recommendations 01/2020, item 75.
[22] EDPB Recommendations 01/2020, item 52.
[23] EDPB Recommendations 01/2020, item 99.

protection of the personal data essentially equivalent to that guaranteed within the EEA".[24]

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'*.[25] 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*".[26]

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

2.4.2.1 Applicable transfer tool

The investigation shows that Dagens Industri and Google have entered into standard data protection clauses (standard contractual clauses) within the meaning of Article 46 of the GDPR 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.

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

[24] EDPB Recommendations 01/2020, item 128.
[25] EDPB Recommendations 01/2020, item 77.
[26] EDPB Recommendations 01/2020, item 79.

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.[27]

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 Dagens Industri

The next question is whether Dagens Industri has taken sufficient additional protective measures.

As data controller and exporter of personal data, Dagens Industri is obliged to ensure that the rules in the GDPR are complied with. 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 by the recipient (Google) and the exporter (Dagens Industri) taken together 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 on 9 April 2021, Google stated that it had taken action.

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

As regards the *legal and organisational measures, it* can be noted that neither information to users of the Tool (such as Dagens Industri), the[28] publication of a transparency report or a publicly available "*government enquiries policy*" prevents or reduces the ability of U.S. intelligence agencies 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 Dagens Industri 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.[29] Thus, such a technical

[27] Paragraphs 184 and 192. Paragraph 259 et seq.
[28] Regardless of whe her such a notification would even be permitted under U.S. law.
[29] See EDPB Recommendations 01/2020, paragraph 81.

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

With regard to Google's action relating to the anonymisation of IP addresses in the form of truncation[30], it is not apparent from Google's response 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.

With regard to the fact that Google LLC has configured the solution so that the JavaScript file is cached in the application cache of the receiving terminal for two hours (which may mean a delay between the first and second call of up to two hours), this means that the calls may have different time stamps, which could in itself amount to an aggravation of the identification of which visitor has made the unique call. IMY notes, however, that Dagens Industri cannot ensure that a delay in the calls actually occurs, partly because it is technically impossible to ensure when (or if) a delay between the first and second call occurs, and when the control (activation) of the caching is beyond the company's control.

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.

2.4.2.3.2 Dagens Industri´s own supplementary measures

Dagens Industri has stated that it has taken supplementary measures in addition to the measures taken by Google. These consist, according to Dagens Industri, that the company has carried out extensive mapping of the life cycle of personal data processed in the Tool and that the company on its own data servers (*transmission through the proxy server)* masks the last octet of the IP address and has the value of the cookies before the data is transferred to Google.[31]

However, IMY considers that these measures are not sufficient for the following reasons.

It is apparent from the company's own data that *two separate* transfers of the individual's IP address are made to Google LLC — *partly* through a call from *the measurement tool "analytics.js"* with the entire IP address exposed and *partly* [32] by

[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 the company's submissions, under the heading 'Additional protective measures taken'.
[32] 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

truncating the last octet when the measured data is transmitted *(and hashing of the cookie value*).[33]

Dagens Industri argues that what can be seen from the first transmission (where the entire IP address is exposed) is only the web page that the IP address has visited and that it is not possible to link the IP address with the page view data etc. which is later measured on the Website. However, IMY notes that the transfer itself involves the transfer of a personal data (IP address), despite the safeguards taken.

With regard to the second transmission, it also contains additional information about the visit to Dagens Industri's website (such as the visitor's device and the time of the visit) and the connection should therefore be made with the IP address as the difference after truncation is only that the last octet is masked, which for IP addresses means only 256 options (i.e. a number between 0-255). Although the masking of the last octet and the "hashing" of the cookie value constitute privacy-enhancing measures, as they limit 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.

Against this background, IMY also finds that the supplementary measures taken by it, 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 Dagens Industri´s 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 invoked by Dagens Industri can provide support for the transfer as set out in Chapter V of the GDPR.

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

IMY therefore concludes that Dagens Industri Aktiebolag violates Article 44 of the GDPR.

3 Choice of intervention

3.1 Applicable provisions

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, orders and administrative fines.

---

that it is still possible to distinguish the IP address from the other IP addresses (255 options), as the IP address can be linked with other transmitted data (e.g. information on the entity and time of visit) to third countries.
[33] See above in section 1.3.17.1, illustration of data flows (p. 8 of the company's opinion).

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 considered 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 an administrative fine, issue a reprimand under Article 58(2)(b) of the Regulation. Account must be taken of aggravating and mitigating factors in the case, such as the nature, gravity and duration of the infringement and the relevant past infringements.

Pursuant to Article 83(5)(c) GDPR, in the event of a breach of Article 44 pursuant to Article 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 previous financial year, whichever is higher, are to be imposed.

3.2 Should an administrative fine be imposed?

IMY has found above that the transfers of personal data to the United States that take place through the Google Analytics tool and for which Dagens Industri is responsible are in breach of Article 44 of the GDPR. Infringements of that provision may, as stated above, give rise to administrative fines. In the present case, it is a serious infringement which should normally be subject to an administrative fine.

When assessing whether a fine should be imposed in this case, account must be taken, in *aggravatingly factor*, of the fact that Dagens Industri has transferred a large amount of personal data to a third country where the data cannot be guaranteed the level of protection afforded in the EU/EEA. The treatment has been carried out systematically and for a long time. Following the Court of Justice of the European Union's judgment of 16 July 2020, the Commission's adequacy decision in the United States[34] changed the conditions for transfers of personal data to the United States. It has now elapsed around 3 years since the judgment was delivered and the EDPB has, during that time, made recommendations on the impact of the public consultation ruling on 10 November 2020 and in final form on 18 June 2021.

In *mitigating factor*, account must be taken of 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. It should also be taken into account in particular that the investigation shows that Dagens Industri has made a serious analysis and mapping of the life cycle of personal-data in the Tool. Dagens Industri has also taken steps such as that the company on its own data servers (transmission through the proxy server) masks the last octet of the IP address (trunking) and has the value of the cookies before the data is transferred to Google. The company has also activated Google's "anonymisation of IP addresses" action by truncation. Dagens Industri has thus taken relatively extensive measures to try to limit the risks to the data subjects and to heal the shortcomings. Dagens Industri

[34] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of he European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield.

has thus also believed that they have succeeded even if the measures in practice have now proved to be not effective.

On a weight of evidence assessment, IMY finds that there is reason to refrain in this case from imposing administrative fine on Dagens Industri for the infringement found and to stay at an order to rectify the deficiency.

3.3 Other interventions

The investigation shows that the transfer measures relied on by Dagens Industri cannot support the transfer under Chapter V of the GDPR. The transfer therefore infringes the Regulation. In order to ensure that the infringement is brought to an end, Dagens Industri shall be ordered pursuant to Article 58(2)(d) of the GDPR to ensure that the Company's processing of personal data in the context of the use of the Google Analytics tool complies with Article 44 and the other provisions of Chapter V. In particular, Dagens Industri ceases to use the version of the Google Analytics tool used on 14 August 2020, unless appropriate safeguards have been taken. 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 advisors [redacted], Head of Legal Affairs, [redacted], Head of Unit, and information security specialist [redacted] have also participated in the final proceedings.