Integritetsskydds myndigheten

Dagens Industri Aktiebolag
Gjörwellsgatan 30
11260 Stockholm

Document number:
DI-2020-11370

Date:
2023-06-30

Decision following supervision under the General Data Protection Regulation - Dagens Industri Aktiebolag'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 Integritetsskyddsmyndigheten finds that Dagens Industri Aktiebolag is processing 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.di.se, thereby transferring personal data to third countries without complying with the conditions laid down in Chapter V of the GDPR.

Pursuant to Article 58(2)(d) of the General Data Protection Regulation, the Swedish Data Protection Authority orders Dagens Industri Aktiebolag to ensure that the company's processing of personal data within the framework of Dagens Industri's use of the Google Analytics tool complies with Article 44 and other provisions of Chapter V. This shall be done in particular by Dagens Industri Aktiebolag 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 has gained legal force.

1 Description of the supervision case

1.1 The organisation

Integritetsskyddsmyndigheten (IMY) has initiated supervision of Dagens Industri Aktiebolag (hereinafter "Dagens Industri" or "the company") following a complaint. The complaint concerns an alleged breach of the provisions of Chapter V of the General Data Protection Regulation linked to the transfer of the complainant's personal data to third countries. The transfer allegedly took place when the complainant visited the company's website, www.di.se ('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 involved have been the authorities in Germany, Norway, Denmark, Estonia and Portugal.

1.2 What is stated in the complaint

The complaint essentially states the following.

On 14 August 2020, the complainant visited the website of Dagens Industri. During the visit, the complainant was logged in to his Google account, which is linked to the complainant's email address. The company 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 terms and conditions of the

[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).

Google's processing of personal data for Google advertising products and also Google's New Order Data Processing Conditions for Google Advertising Products, Google processes personal data on behalf of the controller (i.e. the company). Google LLC is therefore to be classified as the company's data processor according to the aforementioned conditions.

During the complainant's visit to the company's website, the complainant's personal data was processed by Dagens Industri, at least the complainant's IP address and data collected through cookies. Some of the data collected was transferred directly to Google. In accordance with paragraph 10 of the terms and conditions on the processing of personal data for Google's advertising products, Dagens Industri 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.

Following the CJEU judgment in Facebook Ireland and Schrems (Schrems II)[2], the company could no longer rely on an adequacy decision for the transfer of data to the US under Article 45 of the GDPR. The company 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.
It is therefore unable to ensure adequate protection of the complainant's personal data when it is transferred to Google.

1.3 What Dagens Industri has stated

Dagens Industri Aktiebolag has mainly stated the following.

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

Dagens Industri has taken the decision to implement the Tool on the Website, which has been done by embedding the code for the Tool on the Website. The Tool is still active. The company is established in Sweden and has not taken such a decision for any other European website.

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 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 may thus be included in the statistics.

[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-

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, you cannot 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 processors or sub-processors of 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 data processors (the Recipients) process the data listed below.

- *Page view data* - such as URL, clicks in menus, articles visited, reading time and how long the visitor watches a video.
- *Technical information about the device* - e.g. cookie value (which is hashed before being 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 indicating whether the visitor is a subscriber or not.[4]
- *So-called "own dimensions"* - e.g. the version of the publishing platform on which a page view occurred, information about the article (e.g. author).
- *IP addresses* - IP addresses are processed when the Google Analytics measurement script is *loaded* and when measured data is *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 managed on an EU-based infrastructure before being sent together with the measured data to the Tool (see more on this below).

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

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

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 economic and business issues. It is not aimed at children or other particularly vulnerable groups.

1.3.5 When the code of the Tool is executed and access is granted to recipients
The code of the Tool's content, i.e. the script that measures the data sent to the Tool, is only executed if the visitor has given his/her consent to Dagens Industri

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

uses analysis 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 measures are implemented, such as anonymisation of the 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 processors and sub-processors will have access to the pseudonymised data stored in the Tool to the extent necessary for the processor or sub-processor to perform the service, including support and troubleshooting services.

1.3.6 How long the personal data is stored

The data measured on the Website and transferred to the Tool is stored in the Tool for 26 months and then deleted. Dagens Industri saves the data to be able to analyse the use of the Website over time, more specifically to be able to make annual comparisons and thereby analyse how the use changes.
Dagens Industri has assessed that it is necessary to at least be able to compare usage over two annual 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 Which countries the personal data is processed in

The data transferred to the Tool is stored, inter alia, in 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 processing agreement with the Supplier, which regulates the Supplier's and its subcontractors' personal data processing.

Since the purposes and means of the processing are entirely determined by Dagens Industri, Google LLC and Google Ireland Ltd are the processors of the personal data processing in relation to the Tool.

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

1.3.9 Ensuring that the processing is not carried out for the recipients' own purposes

1.3.9.1 In general

Dagens Industri is committed to using only such suppliers who can fulfil the company's high requirements for secure and legal personal data processing. Before a particular supplier is selected, 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 where the company intends to conduct audits of the most important suppliers, based on a rolling schedule. Dagens Industri also maintains a continuous dialogue with Google, where security and data protection issues are discussed.

1.3.9.2 Contract with the Supplier

Through the subcontract with the Supplier and the documented instructions provided by Dagens Industri in this regard, it has been contractually ensured that the Supplier and its subcontractors do not process personal data for their own or other purposes.

third party purposes. The assistance agreement thus contains specific 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 Data Processing Agreement clarifies that the Supplier under no circumstances is entitled to process personal data for its own purposes.

As an incentive to comply with the requirements set out in the assistance agreement and to emphasise its importance, the Supplier has an obligation to compensate Dagens Industri if the Supplier should breach the agreement or applicable data protection legislation and this results in 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 takes place in accordance with Dagens Industri's documented instructions and applicable data protection legislation.

In the event that Dagens Industri has reason to assume that the Supplier does not comply with the requirements set out in the assistance agreement, Dagens Industri intends to conduct such an audit. The Supplier is also entitled to request documentation and conduct audits in relation to Google (section 7.5 of Google's assistance agreement).

Dagens Industri may also request an audit of Google's systems and procedures in accordance with the assistance 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, on how the Website is used, and make analyses based on this data.
Web statistics can show, for example, which pages are the most visited, which path visitors take through the website, and from which pages visitors leave the website. Web analytics can also provide insight into visitor frequency and which content is visited for the longest time. The analyses made using the Tool can, for example, form the basis for product improvements.

1.3.11 Own verifications of transfers affected by the Schrems II judgment
Following the publication of the Schrems II judgment on 16 July 2020, Dagens Industri launched a project at the end of July 2020 to generally identify transfers of personal data to third countries. The project was not specific to the Tool, but concerned
third country transfers in general. In connection with Dagens Industri becoming aware of, among other things, the complaint in question, a project was initiated on 18 August 2020 that specifically concerned the use of the Tool. Relatively immediately after the judgment, the company was able to establish that it is relevant to the data transfer that takes place within the framework of the Tool and Dagens Industri has subsequently taken relevant protective measures, see below.

1.3.12 Transfer tools under Chapter V of the GDPR
Dagens Industri has entered into a data processing agreement directly with Google LLC. Google's standard contractual clauses are part of the data processing agreement. The Data Processing Agreement states that Google is bound by the clauses (clause 10.2). The clauses are based on Commission Decision 2010/87/EU for transfers from an EU/EEA controller to a non-EU/EEA processor. These terms and conditions apply automatically upon conclusion of the Google data processing agreement and thus do not need to be signed separately to be applicable. This is stated in the preamble to

Under Swedish law, which applies to the standard contractual clauses, this means that they become part of the contract.

Google's standard contractual clauses also form part of the data processing agreement with the Supplier in accordance with Annex 2 of the data processing agreement with the Supplier.

Dagens Industri has also entered into a personal data processing agreement with the Supplier, where Google Ireland Ltd acts as sub-processor and which in turn has certain sub-processors in third countries. Also in this agreement, Google's standard contractual clauses are applied as transfer tools.

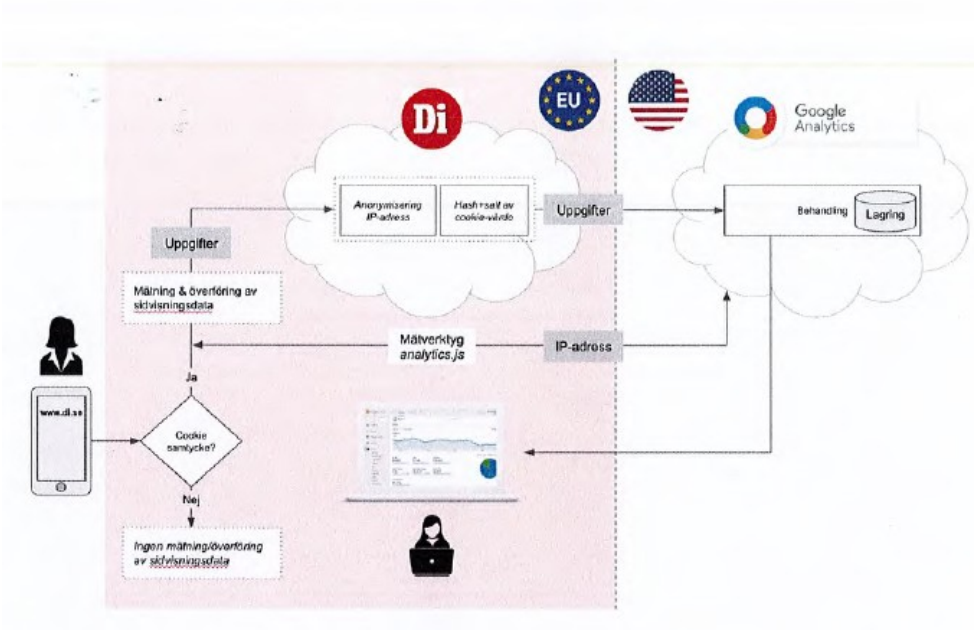
1.3.13 Checking obstacles to enforcement in third country legislation

Dagens Industri has not yet been able to determine with certainty whether there is anything in third country legislation that prohibits recipients from fulfilling their contractual obligations under the standard contractual clauses. As a precautionary measure, the company has therefore assumed that this is the case and has taken special technical protection measures to ensure that the protection of the data processed in the Tool reaches an acceptable level.

1.3.14 Additional protection measures taken in addition to those taken by Google

1.3.14.1 Introduction

Dagens Industri has carried out a detailed mapping of the life cycle of personal data processed in the Tool, and has identified and implemented a number of additional safeguards. These measures are visualised in the image below, and are further commented on in the following sections.



1.3.14.2 Control over the collection and transfer of data to the Tool

A common way of using the Tool, unless additional safeguards are taken, is to transfer the data measured by the Website's measurement script directly to the Tool's servers, without first passing through a checkpoint of the controller using the Tool.

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

Dagens Industri has taken protective measures before data is transferred to the Tool. To take control of what data is transferred to the Tool's servers outside the EU/EEA, the company has implemented technical measures that mean that the data collected via the Google Analytics measurement script on the Website is initially transferred to a proxy server located within the EU where the data is processed to avoid it being used to identify an individual thereafter. The software used is 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 only used as a rented infrastructure to run the proxy server's code. The data processed on the GCP takes place exclusively at data centres within the EU. Dagens Industri is the data controller for the processing that takes place in the proxy server.

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

1.3.14.3 Anonymisation of IP address and algorithm

The data that can in some cases be linked to an individual and that is transmitted from the website to the proxy server is the IP address and cookie value. The examples below illustrate how these numbers may look before and after being processed on the proxy server.

Before processing on proxy server: Data

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

Before transmitting measured data to the Tool, the proxy server performs the following:

- *Anonymisation of IP address*. The visitor's IP address is anonymised through generalisation and aggregation where the last octet of the IPv4 address is replaced with ".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 pseudonymised personal data (when the company can link the cookie value to data in its other systems). As an additional safeguard before transmission to the Tool, the cookie value from the visitor's client is hashed with a "salt".[6] The hashing of the cookie value provides additional protection against

[5] 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).
[6] See information on "Keyed-hash function with stored key" in the WP29 guidance on anonymisation techniques.

the risk that US authorities may link "intercepted data" (i.e. data that could potentially be read by signals intelligence programmes either "at rest" in the Tool or "in transfer") with identifying data that could potentially be accessed by US authorities by other means.

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

Tasks

- 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 this is to be transmitted together with the measured page view data etc. (see above for which data points are measured).

Previously, the IP address was exposed to the Tool when the Google Analytics measurement script was read into the visitor's browser via encrypted transmission from the Tool's server. It is not possible to connect the IP address with the page view data etc. that is measured on the Website at a later date. Dagens Industri has therefore assessed that this exposure of the IP address does not constitute a privacy risk for visitors to the Website.

Although Google LLC can indirectly deduce the time of the visit to the website, this possibility is very limited. Google has configured the server on which "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 the website from which it is first retrieved (i.e. not necessarily on the Website).
During this time period, no more calls are made where 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 has a temporally corresponding machine log at 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 at work and/or during the previous two hours visited another website that uses Google Analytics (most likely given that about 74% of the world's 10,000 most popular websites are present) means that a large proportion of visits to the Website only result in transmitted page view data from Dagens Industri's proxy server and no loading of the Tool with associated transmission of IP address. This greatly complicates any attempts to link machine logs from the transfer of the Tool and transferred page view data from Dagens Industri's proxy server and, according to Dagen, reduces the risk to beyond "reasonable probability".

1.3.14.4 More on verification that additional measures can be implemented *in practice, etc.* Dagens Industri's considerations regarding the measures it has implemented are based on the EDPB's recommendations on how to assess individual third country transfers in their specific legal context (paragraph 33).[7]

The security measures consist mainly of the responsibility and control taken by Dagens Industri over the phases of the life cycle before the transfer of the data to the Tool. The risk assessment has been based on the premise that the protection of data subjects is best achieved by disconnecting the data transferred outside the EU/EEA from the data subject and their technical device used to access the Website, and that the company controls the process that ensures that these measures are carried out.

1.3.14.5 Dagens Industri's conclusion on the adequate level of security protection
Taking into account the measures implemented, Dagens Industri assesses that the risk that the integrity or rights of the data subjects would be violated through the use of the Tool is very small. The company's overall assessment is thus that a sufficient level of protection is achieved through the implemented measures.

1.3.15 Dagens Industri's assessment and conclusion on whether the data can be considered identifiable

1.3.15.1 The company's assessment regarding whether the data can be considered identifiable Dagens Industri considers that it is not obvious that an assessment leads to the data in question - IP address, certain system information and visited web address - constitutes personal data.

Recital 26 of the GDPR states, inter alia, the following:

'To determine *whether a natural person is identifiable, account should be taken of any means, such as screening, which, either by the controller or by another person, could reasonably be used to directly or indirectly identify the natural person. To determine whether means are reasonably likely to identify the natural person, all objective factors, such as the costs and time taken for identification, should be taken into account, taking into account the technology available at the time of the processing as well as technological developments.*"

The Article 29 Working Party in its guidance[8] on the concept of personal data has further clarified the assessment process:

Recital 26 of Directive 95/469 (repealed) pays particular attention to the term 'identifiable' when it states that '*in determining whether a person is identifiable, account should be taken of all the means likely to be reasonably used either by the controller or by any other person to identify the person'. This means that a purely hypothetical possibility to identify the individual is not sufficient to consider the person as "identifiable". If this possibility, taking into account "any means reasonably likely to be used by the controller or any other person", does not exist or is negligible, the person should not be considered "identifiable" and the information would not be considered "personal data". The criterion "any means by which*

[7] EDPB Recommendations 01/2020 on measures complementary to transfer tools to ensure compliance with the EU level of personal data protection Version 2.0 Adopted on 18 June 2021.
[8] WP 136, Article 29 Working Party Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007.
[9] Directive 95/46/EC of the European 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.

reasonably likely to be used either by the controller or by any other person" should take into account in particular all the factors at stake.
The cost of implementing identification is one factor, but not the only one. If the data is intended to be stored for one month, identification cannot be expected to be possible during the "lifetime" of the information and it should not be considered as personal data."[10]

Furthermore, the guidance states that

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

1.3.15.2 The company's conclusion regarding whether the *data can be considered to* be identifiable Dagens Industri has concluded that in order for it to be personal data under the GDPR, the assessment of whether individuals are identifiable must be based on all relevant circumstances and assess the reasonable likelihood of identification, of which the purpose of the processing is a circumstance. As the purpose of the processing is not to identify individuals, technical safeguards are an additional important factor in assessing whether individuals are likely to be identified.

Against this background, Dagens Industri concludes that it is not obvious that an assessment in accordance with the Article 29 Working Party's guidance leads to the data in question - IP address, certain system information and visited web address - constituting personal data.

The assessment that individuals are not identifiable has been made taking into account the circumstances set out in (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 constitutes technical protection measures. According to Dagens Industri, it is by no means obvious that an assessment in accordance with the guidance leads to the data in question - IP address, certain system information and visited web address - constituting personal data.

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. Dagens Industri has been given the opportunity to comment on Google LLC's statement. Google LLC'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. Subsequently, the Tool performs the tracking operation, which consists of collecting information related to the call in various ways and sends the information to the Tool's servers.

[10] WP 136; Article 29 Working Party Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, page 15.
[11] WP 136; Article 29 Working Party Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, pages 16 and 17.

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 settings of the tag manager. The integrator of the Tool can make various settings, such as the storage 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 requests 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 that in the code

for the Tool to enable IP anonymisation, which means that IP addresses are truncated and contribute to data minimisation. If the IP anonymisation service is fully used, the IP address is anonymised 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.

2 Justification of the decision

2.1 The framework of the audit

Based on the complaint in the case, IMY has only reviewed 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 Data Protection Regulation. The supervision does not include whether the company's personal data processing is otherwise compatible with the data protection regulation.

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 GDPR, personal data is "*any information relating to an identified or identifiable natural person ('data subject'), whereby an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data 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.[12]

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.[13] Furthermore, Recital 26 of the GDPR states that in order to determine whether a natural person is identifiable, any means, such as 'singling out', that 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 with *reasonable*

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

likely to be used to identify the natural person, all objective factors, such as the costs 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.

The Article 29 Working Party has clarified in its 2007 opinion what they consider to be the means reasonably likely to be used for identification, including IP addresses.[14] The opinion states that *all the means reasonably likely to be* used for identification include the cost of carrying out the identification, the intended purpose, the structure of the processing and technical errors. On the other hand, account should be taken of the state of the art at the time of the processing and the development possibilities during the period in which the data will be processed, the factors are thus dynamic and may change over time.

The wording of Recital 26 of Directive 95/46 suggests, by referring to all means *reasonably* likely to be used by the controller or another person, that it is not required that a single person holds all the information necessary to identify the data subject.[15]

The 2007 Article 29 Working Party Opinion states in example number 15 the following about dynamic IP addresses on a computer located at an Internet café where no identification is required to use the Internet. [It could be argued that the data collected regarding the use of computer X over a certain period of time does not allow the user to be identified by reasonable means and is therefore not personal data.[16]

In Breyer, the CJEU ruled that a person is not considered identifiable from a particular piece of data if the risk of identification is negligible in practice, which it is if identification of the person concerned is prohibited by law or impossible in practice.[17] However, in M.I.C.M. of 2021 and in Breyer, the CJEU ruled that dynamic IP addresses constitute personal data in relation to the person processing them, where that person also has the legal possibility of identifying the holders of the internet connections by means of the additional information available to third parties.[18]

[14] Opinion 4/2007 on the concept of personal data, 01248/07/SV WP 136, page 16.
[15] ECJ judgment Breyer, C-582/14, EU:C:2016:779, paragraph 43.
[16] Opinion 4/2007 on the concept of personal data, 01248/07/SV WP 136, pages 17 and 18.
[17] ECJ judgment Breyer, C-582/14, EU:C:2016:779, paragraphs 45-46.
[18] 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.

2.2.2 The assessment of the Data Protection Authority

To determine whether the data processed through the Tool constitutes personal data, IMY shall consider whether Google or Dagens Industri, through the implementation of the Tool, can identify individuals, e.g. complainants, when visiting the Website or whether the risk of this is negligible.[19]

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

The investigation shows that Dagens Industri implemented the Tool by inserting a JavaScript code (a tag), specified by Google, into the source code of the Website. While the page is loading in the visitor's browser, the JavaScript code from Google LLC's servers is uploaded and executed locally in the visitor's browser. At the same time, a cookie is set 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 access the Website and a unique identifier identifying the company (i.e. the company's Google Analytics account ID).
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. Although 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 may 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) which result in data constituting personal data, notwithstanding the fact that the IP address is not transmitted in its entirety.

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 singling out (through the word "screening" in recital 26 of the GDPR) is in itself sufficient to make the visitor indirectly identifiable. It is also not required that Google or Dagens Industri 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 be reasonably used by* either the controller or the complainant to identify the visitor.

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

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* are 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.[20] IP addresses do not lose their character as personal data merely 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. Although the truncation[21] of the last octet and the hashing of the cookie value are privacy enhancing measures, as they limit the scope of the data that can be accessed by authorities (in third countries), IMY notes that it is still possible to link the transmitted data to other data also transmitted to Google LLC (to the US). This allows for identification, which in itself is sufficient for the data to collectively constitute personal data.

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 - like dynamic IP addresses - the data cannot be directly attributed to a specific data subject without the use of additional data. 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, which is guaranteed by Article 8 of the GDPR.

[20] 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.
[21] 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.

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 broad scope of application of data protection rules as recognised by the CJEU case law.[22]

Furthermore, because the complainant was logged in to his Google account when he visited the website, Dagens Industri processed data from which it was possible to draw conclusions about the individual based on his registration with Google. It follows from Google's statement that implementing 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 tracing the individual through his or her 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 constitutes processing of personal data.

2.3 Dagens Industri is the data controller for the processing

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

The answers provided by Dagens Industri show that it has made the decision to implement the Tool on the Website. Furthermore, it appears that Dagens Industri's purpose with the implementation of the tool has been that the company should be able to analyse how the Website is used, and in particular be able to follow the use of the Website over time.

IMY finds that by deciding to implement the Tool on the Website for the said purpose, Dagens Industri has established the purposes and means of the collection and subsequent processing of these personal data. Dagens Industri is therefore the data controller for this processing.

[22] 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.

2.4 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 Dagens Industri'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, which is 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, fulfil the conditions set out in Chapter V. All the provisions of that chapter must be applied in order to ensure that the level of protection guaranteed 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 adequacy decision that previously applied to the transfer of personal data to the US.[23] 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 pursuant to Article In accordance with Article 45(3), a controller or processor may transfer personal data to a third country only after having implemented appropriate safeguards, and on condition that legal 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 this 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 is 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, this is *"inter alia*

[23] 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.

the case where the law of that third country authorises the authorities of that third country to interfere with the rights of data subjects in relation to those data."[24]

The reason why the CJEU annulled the adequacy decision with the US was because of the way in which US intelligence agencies can access personal data. According to the Court, the conclusion of standard contractual clauses cannot in itself ensure a 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".*[25]*

The recommendations of the European Data Protection Board (EDPB) on the implications of the judgement[26] 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 as regards its laws and practices applicable to the transfer"*.[27]

The EDPB recommendations indicate that such additional safeguards can be divided into three categories: contractual, organisational and technical.[28]

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 [...]".[29]*

With regard to *organisational* measures, *the* EDPB stresses that "*selecting and implementing one or more of these measures will not necessarily and systematically ensure that [a] transfer meets the basic equivalence standard that*

---

[24] points 125-126.
[25] point 133.
[26] 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").
[27] EDPB Recommendations 01/2020, paragraph 75: IMY translation.
[28] EDPB Recommendations 01/2020, paragraph 52.
[29] EDPB Recommendations 01/2020, paragraph 99; IMY translation.

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 substantially equivalent to that guaranteed in the EU/EEA*".[30]

With regard to *technical* measures, the EDPB points out that "*these measures will be necessary in particular when the legislation of that country imposes on the importer obligations 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*".[31] 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 authorities from identifying data subjects, drawing conclusions about them, identifying them in another context or linking the transferred data to other datasets that may include, inter alia, network identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts*".[32]

2.4.2 The assessment of the Data Protection Authority

2.4.2.1 Applicable transfer tool

The investigation shows that Dagens Industri and Google have concluded standardised data protection clauses (SCCs) 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.

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.

---

[30] EDPB Recommendations 01/2020, paragraph 128; IMY translation.
[31] EDPB Recommendations 01/2020, paragraph 77; IMY translation.
[32] EDPB Recommendations 01/2020, paragraph 79; IMY translation.

In Schrems II, the CJEU found 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 legal remedy.[33]

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 protective measures implemented by Google and Dagens Industri

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

As a data controller and exporter of personal data, Dagens Industri is obliged to ensure compliance with the rules of the General Data Protection Regulation. This responsibility includes, among other things, in each individual case, when transferring personal data to third countries, assessing which additional protection measures should be used and to what extent, including evaluating whether the measures taken by the recipient (Google) and the exporter (Dagens Industri) 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 put in place by Dagens Industri and Google LLC are effective, in other words, prevent US intelligence agencies from accessing 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),[34] the publication of a transparency report, nor a publicly available "*policy for handling government requests*" prevents or reduces the ability of US intelligence agencies to access the personal data. In addition, 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.

With regard to the *technical measures* taken, neither Google LLC nor Dagens Industri have 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 under the US regulatory framework.

---

[33] Paragraphs 184 and 192; paragraph 259 et seq.
[34] Regardless of whether such notification would even be allowed under US law.

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, is nevertheless under an obligation to grant access to or provide imported personal data held by Google LLC, including any encryption keys necessary to make the data intelligible.[35] 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 argument that *'to the extent that Google Analytics measurement information transmitted by website owners constitutes personal data, it may be considered to be pseudonymised', it should 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 of combining unique identifiers with other data (e.g. metadata from browsers or devices and the IP address) and the possibility of linking such information to a Google account for logged-in users makes individuals identifiable.

As regards Google's action regarding the anonymisation of IP addresses in the form of truncation[36], it is not clear from Google's response whether that 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 there is no potential access to the entire IP address before the last octet is truncated.

Regarding the fact that Google LLC has configured the solution so that the JavaScript file is cached in the receiving terminal's application cache for two hours (which can mean a delay between the first and second call of up to two hours), this means that the calls can have different time stamps, which in itself could make it difficult to identify which visitor has made the unique call. However, IMY notes that Dagens Industri cannot ensure that a delay of 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 because the control (activation) of the caching is outside the company's control.

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 services to access the personal data or render such access ineffective.

2.4.2.3.2 Dagens Industri's own additional safeguards

Dagens Industri has stated that the company has taken further protective measures in addition to the measures taken by Google. According to Dagens Industri, these consist of the fact that the company has carried out extensive mapping of the life cycle of personal data processed in the Tool and that the company masks the last octet of the IP address on its own data servers (*transmission through the proxy server)* and hashes the value in the cookies before the data is transferred to Google.[37]

---

[35] See EDPB Recommendations 01/2020, paragraph 81.
[36] 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).
[37] See above in the section on what the company has stated, under the heading "Additional protective measures taken".

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

It is clear from the company's own information that *two separate* transfers of the individual's IP address take place to Google LLC - *firstly* by a call from the *measurement tool "analytics.js"* with the entire IP address exposed, and *secondly* by truncation[38] of the last octet when measured data is transferred *(and hashing of the cookie value*).[39]

Dagens Industri claims that what can be deduced from the first transfer (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. that is measured on the Website at a later date. However, IMY notes that the transfer in itself constitutes a transfer of personal data (the IP address), despite the protective measures taken.

As regards the second transmission, it also contains additional information about the visit to the Dagens Industri website (such as the visitor's device and the time of the visit) and the link should therefore be able to 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). Even if 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 still possible to link the transferred data to other data that is also transferred to Google LLC.

Against this background, IMY concludes that even the additional measures taken by the company, 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 to render such access ineffective.

2.4.2.3.3 Conclusion of the European Data Protection Authority

IMY finds that the measures taken by Dagens Industri and Google are neither individually nor collectively effective enough to prevent US intelligence agencies from accessing the personal data or to render such access ineffective.

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

IMY therefore finds that Dagens Industri Aktiebolag is in breach of Article 44 of the GDPR.

---

[38] 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.

[39] See above in section 1.3.17.1, illustration of data flows (p. 8 of the company's statement).

3 Choice of intervention

3.1 Legal regulation

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

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 should 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.

Article 83(5)(c) of the GDPR provides that an infringement of Article 44 in accordance with 83(2) is 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.

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 Dagens Industri is responsible are contrary to Article 44 of the General Data Protection Regulation. Violations of that provision can, as stated above, lead to penalties. In this case, it is a question of a serious offence that should normally lead to a penalty fee.

When assessing in this case whether a penalty should be imposed, the fact that the offence has been committed by Dagens Industri transferring a large amount of personal data to third countries where the data cannot be guaranteed the level of protection provided in the EU/EEA must be taken into account as an *aggravating factor.* The processing has been carried out systematically and over a long period of time. After the Court of Justice of the European Union (CJEU) ruled on 16 July 2020 against the Commission's decision on adequate protection in the United States[40], the conditions for transfers of personal data to the United States changed. Approximately 3 years have now elapsed since the judgment was delivered, during which time the EDPB has provided recommendations on the implications of the judgment for public consultation on 10 November 2020 and in final form on 18 June 2021.

[40] 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.

In *mitigation,* the specific situation that arose after the judgment and the interpretation of the EDPB's recommendations, where there was a gap after the transfer tool to the United States was rejected by the European Court of Justice in accordance with the Commission's previous decision, should be taken into account. It should also be noted 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 measures such as the company masking the last octet of the IP address (truncation) on its own data servers (transmission through the proxy server) and hashing the value in the cookies before the data is transferred to Google. The company has also activated Google's measure "anonymisation of IP addresses" through truncation. Dagens Industri has thus taken relatively extensive measures to try to limit the risks to data subjects and to remedy the shortcomings. As a result, Dagens Industri has also believed that it has succeeded, even though in practice the measures have now proved to be ineffective.

In an overall assessment, IMY finds that there is reason in this case to refrain from imposing a penalty fee on Dagens Industri for the established infringement and to stop at an order to remedy the deficiency.

3.3 Other interventions

The investigation shows that the safeguards for transfer invoked by Dagens Industri cannot support the transfer under Chapter V of the GDPR. The transfer thus constitutes an infringement of the Regulation. In order to ensure that the infringement ceases, Dagens Industri shall be ordered under Article 58(2)(d) of the GDPR to ensure that the company's processing of personal data within the framework of the use of the Google Analytics tool complies with Article 44 and other provisions of Chapter V. This shall be done in particular by Dagens Industri ceasing to use the version of the Google Analytics tool used on 14 August 2020, unless adequate safeguards have been taken. The measures shall 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)

4 Appeal reference

4.1 How to appeal

If you want to appeal the decision, you should write to the Authority. Specify in your letter the 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.