Integritetsskydds myndigheten

Tele2 Sverige Aktiebolag
Box 62
16494 Kista

Document number:
DI-2020-11373

Date:
2023-06-30

Supervisory decision under the General Data Protection Regulation - Tele2 Sverige AB's transfer of personal data to third countries

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 Tele2 Sverige Aktiebolag is processing 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.tele2.se during the period from 14 August 2020 to May 2023, thereby transferring personal data to third countries without fulfilling the conditions laid down in Chapter V of the GDPR.

Pursuant to Article 58(2) and 83 of the GDPR, IMY decides that Tele2 Sverige Aktiebolag shall pay an administrative fine of SEK 12 million (twelve million) for infringement of Article 44 of the GDPR.

1 Description of the supervision case

1.1 The organisation

The Integritetsskyddsmyndigheten (IMY) has initiated supervision of Tele2 Sverige Aktiebolag ('Tele2' or 'the company') following a complaint. The complaint concerns an alleged 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.tele2.se ('Tele2'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 process at IMY has been carried out by correspondence.

1.2 What is stated in the complaint

The complaint essentially states the following.

On 14 August 2020, the complainant visited Tele2's website. 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 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 its website, Tele2 processed the complainant's personal data, at least the complainant's IP address and data collected through cookies. Some of the data collected was transferred directly to Google. I

[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).

In accordance with paragraph 10 of the terms and conditions on the processing of personal data for Google's advertising products, Tele2 has authorised Google to process personal data of the complainant in the United States. Such data transfer requires a legal basis in accordance with Chapter V of the GDPR.

Following the CJEU judgement 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 Tele2 has stated

Tele2 Sverige Aktiebolag has essentially stated the following.

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

Tele2 has made the decision to implement Google Analytics (the "Tool") on the Website, which has been done by embedding the code for the Tool on the Website. The Company began to phase out the version of the Tool covered by IMY's supervision in the spring of 2022 and stopped using that version in June 2023 but has not been able to provide an exact date for this. The company is established in Sweden and has not made such a decision for any other European website.

The purpose of using the Tool is to compile and analyse statistics on visits to the Website.

The statistics on visits to the Website obtained through the Tool have been evaluated only by Tele2 in Sweden.

There is no option in the Tool's settings to make choices regarding the transfer of data to the US.

1.3.2 Recipients of the data

As part of Tele2's use of the Tool on the Website, information is disclosed to a number of parties, all of whom are processors or sub-processors of the company, including Google LLC, Google Ireland Ltd and their sub-processors.

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

1.3.3 The data processed in the Tool and what constitutes personal data

The information processed by Tele2 and Google in the context of the Tool includes (i) information about the visit to the Website such as the pages viewed or clicks made, (ii) information about the device accessing the Website and (iii) information in the cookie (_ga cookie) consisting of the Client ID.

Tele2 uses the Tool to analyse statistics regarding visits to the website www.tele2.se. All statistics and reports generated through the Tool are produced at an aggregated level and cannot be used to directly or indirectly identify any natural person.

The production of statistics and reports via the Tool is made possible by the use of cookies on the Website. If a visitor to the Website has consented to the use of cookies, a cookie is placed in the visitor's browser. The information processed through the use of the Tool thus consists of the following categories:
(i) information about the visit to the Website such as the pages viewed or clicks made, (ii) information about the device visiting the Website and (iii) information in the cookie (_ga cookie) consisting of the Client ID.

(i) Information about the visit to the Website
Information regarding the visit to the Website does not in itself contain any information that can be used to directly or indirectly identify any natural person, i.e. a page view or a click constitutes in itself completely anonymous information.

(ii) Information about the entity visiting the Website
Information about the device that calls and visits the Website consists, for example, of the type of browser and the IP address used during the visit. Regarding IP addresses, static IP addresses are now only used by a few companies and organisations. Otherwise, dynamic IP addresses are used exclusively for all consumers. In simple terms, a dynamic IP address means that a device is assigned an IP address every time it connects to the internet, and the device is then assigned completely new IP addresses on subsequent connections. A device is not necessarily a computer, mobile phone or tablet but can in many cases consist of a router or other device to which several computers, mobiles or tablets then connect, and the IP address can thus not be attributed to the computer, mobile phone or tablet but to the router.
In order to indirectly identify a person by means of a dynamic IP address, it is necessary to supplement it with a time of use and to obtain additional information on the identity of the IP address from the visitor's internet service provider.

The Tool uses IP address only for the purpose of analysing statistics relating to visits to a website. For that purpose, a user of the Tool should not have any legal means under Swedish law to obtain the additional information necessary to indirectly identify a natural person.

Furthermore, the IP address collected by the Tool is anonymised almost immediately after collection by replacing the digits after the last point of the IP address with 0 (e.g. 192.169.0.100 becomes 192.168.0.0). Such IP anonymisation is done at the earliest possible stage of the collection process and the full IP address is never stored or processed on disk. For more information on anonymisation

of IP address in the Tool, see https://support.google.com/analytics/answer/2763052?hl=en.

Anonymisation of the IP address thus means that the user of the Tool never has access to the full IP address and there are no means that a user of the Tool can reasonably use to indirectly identify a natural person (cf. recital 26 of the GDPR) with the result that the risk of identification can be considered negligible in practice.

(iii) Information in the _ga cookie
The information processed through the use of the _ga cookie is a Client ID. The Client ID is a random number with a time stamp that is stored in the _ga cookie. This Client ID can be used to see whether a browser has previously connected to the Website. However, Tele2 cannot use the Client ID individually or together with an anonymised IP address to directly or indirectly identify a natural person.

Due to the above, Tele2 considers that it can be questioned whether Tele2 processes and transfers personal data to third countries at all. Considering that some uncertainty may be considered to exist regarding the legal assessment of the above-mentioned circumstances, Tele2 has, for reasons of caution, chosen to apply the rules of the GDPR to the data processed within the framework of the Tool.

1.3.4 Categories of persons concerned by the processing
The data relate to visitors to the Website. No special categories of personal data as defined in Article 9(1) of the GDPR are processed within the Tool. Tele2 cannot use the Tool to identify different categories of persons visiting the Website. The Website is not aimed at children, or any other special category of data subjects, and visitors to the Website are not required to indicate any age, or any other personal data processed in the Tool.

1.3.5 When the code of the Tool is executed and recipients are given access, the Tool is activated and cookies are placed in the user's browser after the visitor has consented to the use of cookies. Anonymisation of the IP address occurs at the earliest possible stage during the collection process and the full IP address is never stored or processed on disk by Google (https://support.google.com/analytics/answer/2763052?hl=en&ref_topic=2919631).

1.3.6 How long the personal data processed is stored
During the use of the Tool, retention periods of up to 26 months can be set in the Tool. If the agreement for the Tool is terminated, Google undertakes under the Data Processing Agreement to delete personal data in the Tool as soon as practicable after the termination of the agreement, but no later than 180 days.

1.3.7 Which countries the personal data is processed in
According to the information Tele2 has received from Google, the visitor's IP address is anonymised at the data centre closest to where the visitor connects from. Under the terms of the agreement with Google, Google may process the data within the framework of the Tool in, for example, the USA.

1.3.8 Tele2's relationship with Google LCC
Tele2 considers Google as a data processor for the processing that takes place within the framework of the Tool, i.e. Google processes the information in the Tool only for

Tele2's behalf. This is also supported by the agreement between Tele2 and Google regarding the Tool and the data processing agreement applicable to the Tool.

1.3.9 Ensuring that the processing is not for the recipients' own purposes
According to clause 5.3 of the data processing agreement with Google, Google may only process personal data in accordance with Tele2's instructions. Tele2's use of the Tool means that IP addresses are anonymised at the earliest possible stage of the collection process and that the full IP address is never stored or processed on disk by Google. This means that Google cannot process the full IP address for its own purposes or those of third parties.

1.3.10 Description of the company's use of the Tool
Tele2 uses the Tool to analyse statistics regarding visits to the Website. All statistics and reports generated through the Tool are produced at an aggregate level and no action is taken in relation to individual visitors to the Website within the framework of the Tool.

1.3.11 Own checks on transfers affected by the Schrems II judgement
Following the Schrems II judgement, Tele2 initiated an internal review of all international data transfers in Tele2's operations. This review has also included the Tool.

Tele2 has had an ongoing dialogue with Google which has meant that since 12 August 2020, the transfer of data to Google in the US has been based on standard contractual clauses for data protection adopted by the Commission. Since the Court of Justice of the European Union in the Schrems II judgement considered that the legislation to which Google is subject in the US does not correspond to the level of protection provided by European data protection law, additional safeguards are necessary when using the standard contractual clauses for data protection adopted by the Commission.

In the dialogue with Google, Tele2 has therefore discussed what additional protection measures can be taken in relation to the Tool. It has then been established that the protection measures used in relation to the Tool are IP anonymisation (which has been activated by Tele2 ever since the Tool was introduced). In addition, Google has ISO270001 certification for the Tool and Google also uses various encryption solutions in connection with the Tool and the transfer of data to the United States.

1.3.12 Transfer tools under Chapter V of the General Data Protection Regulation
To the extent that personal data is transferred to the United States, the transfer is based on Article 46(2)(c) of the GDPR (Standard Contractual Clauses for data protection adopted by the Commission). The Standard Contractual Clauses apply to the data transfer in the Tool. The Standard Contractual Clauses are not signed by the parties but are included as part of the Data Processing Agreement with Google by reference to these Standard Contractual Clauses in clause 10.2 of the Data Processing Agreement.

1.3.13 Verification of obstacles to enforcement in third country legislation
The EDPB's Recommendation 01/2020 states, inter alia, that pseudonymisation and anonymisation are additional safeguards that can be taken to achieve a level of protection equivalent to that in Europe and thus enable the transfer of personal data to the US based on standard contractual clauses for data protection adopted by the Commission.

Tele2's assessment, based on the additional safeguards used in connection with the Tool, is therefore that the data is adequately protected and that the level of protection is then equivalent to that provided by European data protection law.

Tele2 has verified that the additional safeguards adopted are practicable and that there is nothing in third country legislation that prevents recipients there from implementing the measures to ensure that the level of data protection of natural persons guaranteed in the EU/EEA is not undermined.

1.3.14 Additional protection measures taken in addition to those taken by Google
Tele2 has set IP anonymisation for the Tool.

1.4 What Google LCC 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.
Tele2 has been given the opportunity to comment on Google's statement. Google's opinion states the following about the Tool.

A JavaScript code is included on a web page. When a user visits (calls) a web page, the code triggers a download of a JavaScript file. The Tool then performs the tracking operation, which consists of collecting information related to the call in various ways and sending the information to the Tool's servers.

A webmaster who has integrated the Tool on his website can send instructions to Google for the processing of the data collected. These instructions are transmitted via the so-called tag manager which 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 request and information about, inter alia, the visitor's browser and operating system. According to Google, an HTTP request for any page contains information about the browser and the device making the request, such as the domain name, and information about the browser, such as the type, reference and language. The tool stores and reads cookies in the visitor's browser to evaluate the visitor's session and other information about the request. Through these cookies, the Tool enables the identification of unique users (UUID) across browsing sessions, but the Tool cannot identify unique users across browsers or devices. If a website owner's website has its own authentication system, the website owner can use the ID feature to more accurately identify a user across all the devices and browsers they use to access the website.

When the information is collected, it is transferred to the Tool's servers. All data collected through the Tool is stored in the United States.

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

Google has put in place contractual and organisational safeguards such as always conducting a thorough assessment of whether a request for access to user data from government authorities can be implemented. These assessments are carried out by lawyers/specialised staff who examine whether such a request complies with applicable laws and Google's guidelines. 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 called "data at rest" in data centres, where user data is stored on a disk or backup media to prevent unauthorised access to the data.

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

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

2 Justification of the decision

2.1 The framework of the audit

On the basis of the complaint in the case, IMY has only examined whether Tele2 transfers personal data to the third country USA in the context of Tele2's use of the Tool and whether Tele2 has legal support for it in Chapter V of the GDPR. The supervision does not cover whether Tele2's processing of personal data is otherwise compatible with the GDPR.

2.2 It is a matter of processing personal data

2.2.1 Applicable provisions, etc.

The application of the GDPR requires the processing of personal data.

Article 1(2) of the GDPR aims to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data.

According to Article 4(1) of the Regulation, personal data 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 may 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.[4]

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

So-called "online identifiers" (sometimes referred to as "online identifiers") - such as IP addresses or information stored in cookies - can be used to identify a user, especially when combined with other similar types of information. According to recital 30 of the GDPR, natural persons can be linked to online identifiers provided by their equipment, such as IP addresses, cookies or other identifiers. This can leave traces which, especially in combination with unique identifiers and other data collected, can be used to profile and identify natural persons.

In Breyer, the CJEU ruled that a person is not considered to be identifiable from a particular piece of information if the risk of identification is negligible in practice, which it is if the identification of the person concerned is prohibited by law or impossible to implement in practice.[6] However, in the 2021 M.I.C.M. judgment and in Breyer, the CJEU ruled that dynamic IP addresses constitute personal data in relation to the person processing them, when that person also has a legal possibility of identifying the holders of the IP addresses.

---

[4] CJEU judgment Nowak, C-434/16, EU:C:2017:994, paragraphs 34-35.
[5] ECJ judgment Breyer, C-582/14, EU:C:2016:779, paragraph 41.
[6] ECJ judgment Breyer, C-582/14, EU:C:2016:779, paragraphs 45-46.

Internet connections using the additional information available to third parties.[7]

2.2.2 The assessment of the Data Protection Authority
In order to determine whether the data processed through the Tool constitutes personal data, IMY will consider whether Google or Tele2, through the implementation of the Tool, can identify individuals, such as the complainant, when visiting the Website or whether the risk of doing so is negligible.[8]

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

reasons. The investigation shows that Tele2 has implemented the Tool by

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

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

1. Unique identifier(s) identifying the browser or device used to access the Website and a unique identifier identifying Tele2 (i.e. Tele2's account ID for Google Analytics).
2. Web address (URL) and HTML title of the website and web page visited by the complainant.
3. Information about the browser, operating system, screen resolution, language setting and the date and time of access to the Website.
4. The complainant's IP address.

During the complainant's visit (as referred to in paragraph 1 above), those identifiers were placed in cookies called '_gads', '_ga' and '_gid' and subsequently transmitted to Google LLC. Those identifiers were created for the purpose of distinguishing individual visitors, such as the complainant. The unique identifiers thus make visitors to the Website identifiable. Even if such unique identifiers (as referred to in paragraph 1 above) would not in themselves be considered to make individuals identifiable, it must nevertheless be taken into account that in the present case those unique identifiers 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 identification (through the word "thinning" in recital 26 of the GDPR) is not necessary.

[7] CJEU judgment M.I.C.M, C-597/19, EU:C:2021:492, paragraphs 102-104 and Breyer, C-582/14, EU:C:2016:779,

paragraph 49.

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

GDPR, 'singling out') is in itself sufficient to make the visitor indirectly identifiable. It is also not required that Google or Tele2 intend to identify the complainant, but the possibility of doing so is in itself sufficient to determine whether it is possible to identify a visitor. Objective means that can *reasonably be used* either by the controller or by someone else are *any means that can reasonably* be used for the purpose of identifying the complainant. Examples of *objective means that can reasonably be used* include the availability of additional information from a third party that would enable the complainant to be identified, taking into account both the technology available at the time of identification and the cost (time) of identification.

IMY notes that the CJEU, in the M.I.C.M. and Breyer judgements, established that dynamic IP addresses constitute personal data in relation to the person processing them, when 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.[9] IP addresses do not lose their character of being personal data simply because the means of identification are held by third parties. The Breyer and M.I.C.M. judgements should be interpreted on the basis of what is actually stated in the judgements, i.e. that if there is a legal possibility to access additional information for the purpose of identifying the complainant, it is objectively clear that there is a "*means reasonably likely to be used*" to identify the complainant. According to IMY, the judgements should not be read in a contradictory way, 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 judgement 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 singling out is in itself sufficient to make the visitor identifiable), was not mentioned in the previously applicable Directive as a method of identifying personal data.

In this context, there are also other data (as described in paragraphs 1 to 3 above) with which the IP address can be combined to enable identification. Google's action of truncating[10] an IP address means that the IP address is still distinguishable, as it can be combined with other data transferred to third countries (to the US). This allows for identification, which in itself is sufficient for the data to collectively constitute personal data.

In addition, several other EU/EEA supervisory authorities have decided that the transfer of personal data to third countries has taken place when using the Tool because it has been possible to combine IP addresses with other data (as described in paragraphs 1 to 3 above), thus allowing for data segregation and IP address identification,

---

[9] CJEU judgment 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.

[10] 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.

which in itself is sufficient to determine that the processing of personal data is involved.[11]

IMY notes that there may also be reasons to compare IP addresses with pseudonymised personal data. According to Article 4(5) of the GDPR, the pseudonymisation of personal data means that the data - like dynamic IP addresses - cannot be directly attributed to a specific data subject without the use of supplementary information. According to recital 26 of the GDPR, such data should be considered as data relating to an identifiable natural person.

A narrower interpretation of the concept of personal data would, according to IMY, undermine the scope of the right to the protection of personal data, guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, as it would allow data controllers to specifically identify individuals together with personal data (e.g. when they visit a certain website) while denying individuals the right to protection against the dissemination of such data about them. Such an interpretation would undermine the level of protection of individuals and would not be compatible with the broad scope of application of data protection rules as recognised by the case law of the Court of Justice of the European Union.[12]

Furthermore, since the complainant was logged in to his Google account when visiting the Website, Tele2 processed data from which conclusions could be drawn about the individual based on his registration with Google. According to Google's statement, the implementation of the Tool on a website makes it possible to obtain information that a user of a Google account (i.e. a registrant) has visited the website in question. Admittedly, Google states that certain conditions must be met for it to receive such information, such as that the user (the complainant) has not deactivated the processing and display of personalised advertisements. Since the complainant was logged in to his Google account when he visited the Website, Google may still have been able to obtain information about the logged-in user's visit to the Website. The fact that it is not clear from the complaint that no personalised ads were displayed does not mean that Google cannot obtain information about the logged-in user's visit to the Website.

IMY finds that, in light of the unique identifiers that can identify the browser or device, the possibility of identifying the individual through his or her Google account, the dynamic IP addresses and the possibility of combining these with additional data, Tele2's use of the Tool on a webpage involves the processing of personal data.

2.3 Tele2 is the data controller for the processing

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

---

[11] The Austrian supervisory authority (Datenschultzbehörde) decision of 22 April 2022 regarding the Google Analytics complaint represented by NOYB with local case number 1354838270, the French supervisory authority (CNIL) decision of 10 February 2022 represented by NOYB and the Italian supervisory authority (Garante) decision of 9 June 2022 regarding the Google Analytics complaint represented by NOYB, local case number 9782890.
[12] 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.

The answers provided by Tele2 show that the company has made the decision to implement the Tool on the Website. Furthermore, it appears that Tele2's purpose in doing so was to be able to analyse how the Website is used, in particular to 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, Tele2 has determined the purposes and means of the collection and subsequent transfer of those personal data. Tele2 is therefore the data controller for this processing.

2.4 Transfer of personal data to third countries

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

The question is therefore whether Tele2's transfer of personal data to the United States is compatible with Article 44 of the GDPR and has a legal basis 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 are to be applied in order to ensure that the level of protection of natural persons ensured by the GDPR is not undermined.

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

In Schrems II, the CJEU annulled the previous adequacy decision for the US.[13] In the absence of an adequacy decision since July 2020, transfers to the US cannot be based on Article 45.

Article 46(1) provides, inter alia, that in the absence of a decision in accordance with Article
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 doing *so, the* CJEU stated that "*[e]ven if there is thus*

[13] 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.

while there are situations in which, depending on the legal situation and the practices in force in the third country concerned, the recipient of such a transfer can ensure the necessary protection of data solely on the basis of the standard data protection clauses, there are other situations in which the provisions of those clauses cannot be a sufficient means of ensuring in practice effective protection of the personal data transferred to the third country concerned." According to the CJEU, that is *"in particular the case where the legislation of that third country authorises the authorities of that third country to interfere with the rights of data subjects in respect of those data."*[14]

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

> 'It therefore follows that the standard data protection clauses adopted by the Commission on the basis of point (c) of Article 46(2) of that regulation are intended solely to provide controllers or their processors established in the Union with contractual safeguards which are applied uniformly in all third countries and thus independently of the level of protection ensured in each of those countries. Since those standardised data protection clauses, by their nature, cannot result in safeguards going 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".*[15]*

The recommendations of the European Data Protection Board (EDPB) on the consequences of the judgement[16] 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".*[17]

The EDPB recommendations indicate that such additional safeguards can be divided into three categories: contractual, organisational and technical.[18]

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 that the nature of contractual measures is such that they cannot generally bind the authorities of that third country as they are not parties to the agreement, these measures may often need to be*

---

[14] points 125-126.
[15] point 133.
[16] 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").
[17] EDPB Recommendations 01/2020, paragraph 75; IMY translation.
[18] EDPB Recommendations 01/2020, paragraph 52.

combined with other technical and organisational measures to provide the required level of data protection [...]".[19]

With regard to *organisational* measures, the EDPB stresses that "*[s]electing and implementing one or more of these measures will not necessarily and systematically ensure that [a] transfer meets the basic equivalence standard required by EU law. Depending on the specific circumstances of the transfer and the assessment of the third country's legislation, organisational measures are required to complement contractual and/or technical measures to ensure a level of protection of personal data that is substantially equivalent to that guaranteed in the EU/EEA*".[20]

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*".[21] The EDPB states that *"the measures set out [in the Recommendations] are intended to ensure that access to the transferred data by public authorities in third countries does not jeopardise the effectiveness of the appropriate safeguards in Article 46 of the GDPR transfer tool. These measures would be necessary to ensure an essentially equivalent level of protection to that guaranteed in the EU/EEA, even if the access by public authorities is in accordance with the law of the importer's country, where such access in practice goes beyond what is necessary and proportionate in a democratic society. The purpose of these measures is to prevent potentially unauthorised access by preventing the authorities from identifying the data subjects, drawing conclusions about them, identifying them in another context or linking the transferred data to other data sets that may include, inter alia, network identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts*".[22]

2.4.2 The assessment of the Data Protection Authority

2.4.2.1 Applicable transfer tool

The investigation shows that Tele2 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. Those clauses are in line with those published by the European Commission in Decision 2021/914 of 4 June 2021 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 the Schrems II judgement, which relates to similar circumstances, is relevant and timely, and can therefore be added to the list.

---

[19] EDPB Recommendations 01/2020, paragraph 99; IMY translation.
[20] EDPB Recommendations 01/2020, paragraph 128; IMY translation.
[21] EDPB Recommendations 01/2020, paragraph 77; IMY translation.
[22] EDPB Recommendations 01/2020, paragraph 79; IMY translation.

basis for the assessment in this case without the need for any further analysis of the legal situation in the US.

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

In Schrems II, the CJEU held that the US surveillance programmes based on 702 FISA, Executive Order 12333 (hereinafter 'E.O. 12333') and Presidential Policy Directive 28 (hereinafter '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.[23]

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 safeguards implemented by Google and Tele2

The next question is whether Tele2 has taken sufficient additional safeguards.

As controller and exporter of the personal data, Tele2 is obliged to ensure compliance with the rules of the GDPR, including assessing in each individual case of transfers of personal data to third countries what additional safeguards should be used and to what extent, including evaluating whether the measures taken by the recipient (Google) and the exporter (Tele2) taken 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 Tele2 and Google LLC are effective, in other words, hinder the ability of US intelligence agencies to access the transferred personal data.

With regard to the *legal and organisational measures, it* can be noted that neither information to users of the Tool (such as Tele2),[24] 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

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

such requests because, 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 Tele2 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.

However, with regard to the encryption technology used - for example, for 'data at rest' in data centres, which Google LLC mentions as a technical measure - Google LLC, as an importer of personal data, still has an obligation to grant access to or transmit imported personal data in its possession, including any encryption keys required to make the data intelligible.[25] Thus, such a technical measure cannot be considered effective as long as Google LLC is able to access the personal data in plaintext.

As regards Google LLC's statement that *"to the extent that Google Analytics measurement information transmitted by website owners constitutes personal data, it may be considered to be pseudonymised*", it can be noted that universal unique identifiers (UUIDs) are not covered by the concept of pseudonymisation in Article 4(5) of the GDPR. Pseudonymisation can be a privacy enhancing technique, but the unique identifiers, as described above, have the specific purpose of distinguishing users and not to serve as protection. In addition, the possibility to combine unique identifiers with other data (e.g. metadata from browsers or devices and the IP address) and the possibility to link such information to a Google account for logged-in users, as described above, makes individuals identifiable.

With regard to Google's "anonymisation of IP addresses" measure in the form of truncation[26], it is not clear from Google's response whether this measure takes place before the transfer, or whether the entire IP address is transferred to the US and truncated only after the transfer to the US. Thus, from a technical point of view, it has not been demonstrated that there is no potential access to the entire IP address before the last octet is truncated.

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

2.4.2.3.2 Tele2's own additional safeguards

Tele2 has stated that it has taken further protective measures in addition to those taken by Google. According to Tele2, these consist of the activation of the function for truncating[27] the last octet of the IP address before the data is transmitted to Google, which means that the last octet is masked.

As stated above in relation to Google's actions, it is not clear from Google's response whether this action takes place before the transfer or whether the entire IP address is transferred to the United States; and

---

[25] See EDPB Recommendations 01/2020, paragraph 81.
[26] 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).
[27] 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).

is truncated only after transmission to the United States. Thus, from a technical point of view, it has not been shown that after the transfer there is no potential access to the entire IP address before the last octet is truncated.

Even if the truncation were to take place before transmission, it is not a sufficient measure, as the truncated IP address can be linked to other data, as noted by IMY in section 2.2.2 above. in the range of 0-255) and because the truncated IP address is distinguishable from other IP addresses, this data can be combined with other data (as described above in section 2.2.2) and allow for identification, which in itself is sufficient to determine whether the data together is personal data. Although the masking of the last octet constitutes a privacy enhancing measure, as it limits the scope of the data that can be accessed by authorities (in third countries), IMY notes that it is still possible to link the transferred data to other data also transferred to Google LLC (in third countries).

Against this background, IMY concludes that the additional measures taken by Tele2 in addition to the additional measures taken by Google are also not sufficiently effective to prevent the possibility for US intelligence agencies to access the personal data or render such access ineffective.

2.4.2.3.3 Conclusion of the European Data Protection Authority
IMY finds that Tele2 and Google's measures are neither individually nor collectively sufficiently effective to prevent US intelligence agencies from accessing the personal data or render such access ineffective.

Against this background, IMY finds that neither standard contractual clauses nor the other measures invoked by Tele2 can support the transfer within the meaning of Chapter V of the GDPR.

With this transfer of data, Tele2 therefore undermines the level of protection of personal data of data subjects guaranteed by Article 44 of the GDPR.

IMY therefore finds that Tele2 Sverige AB infringed Article 44 of the GDPR at least during the period from 14 August 2020 until May 2023.

3 Choice of intervention

3.1 Legal regulation

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

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

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

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

The EDPB has adopted guidelines on the calculation of administrative fines under the GDPR which aim to create a harmonised methodology and principles for the calculation of fines.[28]

3.2 Should a penalty be imposed?

IMY has found above that the transfers of personal data to the United States via the Google Analytics tool, for which Tele2 is responsible, infringe Article 44 of the GDPR. Infringements of that provision are subject to penalties under Article 83.

Given, inter alia, that Tele2 has transferred a large amount of personal data, that the processing has been ongoing for a long time and that the transfer has meant that the personal data could not be guaranteed the level of protection provided in the EU/EEA, this is not a minor infringement. A penalty payment should therefore be imposed on Tele2 for the infringement found.

3.2.1 What is the amount of the penalty?

In determining the maximum amount of a fine to be imposed on an undertaking, the definition of an undertaking used by the Court of Justice of the European Union for the purposes of Articles 101 and 102 TFEU (see recital 150 of the GDPR) should be used. According to the Court's case-law, this includes any entity engaged in an economic activity, irrespective of its legal form and the way in which it is financed, and even if the entity is legally composed of several natural or legal persons.[29]

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

IMY assesses that the company's turnover to be used as a basis for calculating the administrative fine is Tele2 Sverige AB's annual report for 2022. The company had a turnover of approximately SEK 28 102 000 000 during that financial year. The maximum penalty fee that can be established in the case is four per cent of this amount, i.e. approximately SEK 1 124 080 000.

In determining the amount of the penalty payment, IMY shall take into account the gravity of the infringement, taking into account both aggravating and mitigating circumstances.

---

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

determine an administrative penalty that is effective, proportionate and dissuasive in the individual case.

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

As regards the assessment of the gravity of the infringement, there are initial factors that justify a more serious approach to the infringement. Tele2 has transferred a large amount of personal data to third countries. The transfer has meant that the personal data could not be guaranteed the level of protection provided in the EU/EEA, which in itself is a serious infringement. In addition, it is aggravating that the transfer of personal data has been going on for a long time, i.e. from 14 August 2020 and is still ongoing, and that they have been systematic. IMY also considers that approximately 3 years have now elapsed since the Court of Justice of the European Union, in its judgment of 16 July 2020, overturned the Commission's adequacy decision in the US[30], thereby changing the conditions for transfers of personal data to the US.

In the meantime, the EDPB has issued recommendations on the consequences of the judgment, which were put out for public consultation on 10 November 2020 and adopted in final form on 18 June 2021. In addition, several other supervisory authorities in the EU/EEA have issued orders to cease the use of the Tool until sufficiently effective security measures have been taken by the controllers. These decisions have included cases where controllers have also taken measures such as "anonymisation of IP addresses" in the form of truncation.[31]

Despite the fact that these recommendations and decisions clearly point to the risks and difficulties in ensuring an adequate level of protection for data transfers to companies in the United States, Tele2 has continued to use the Tool during the period from 14 August 2020 until at least May 2023 without taking its own additional safeguards.
Google's action on IP address truncation[32] means that the IP address is still distinguishable, as it can be linked to other data transferred to third countries (to the US). This enables identification, which means that the data together constitute personal data.

Tele2 is one of the major players in the telecoms industry in Sweden. It concerns data relating to a large number of data subjects who can be identified indirectly and whose data can be linked to other data relating to them. As regards the nature of the data, it already follows from Tele2's own purpose of the processing - i.e. to be able to draw conclusions about how the data subjects navigate on and find their way to the Website - that the data, taken as a whole, makes it possible to draw relatively precise conclusions about the private life of the data subjects and to map them, such as what they buy and what services they are interested in over time and with the company. Tele2's processing of personal data poses risks of serious offence

[30] 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 protection provided by the EU-US Privacy Shield.
[31] Austria's supervisory authority (Datenschultzbehörde) decision of 22 April 2022 regarding the complaint Google Analytics represented by NOYB with local case number 1354838270, France's supervisory authority (CNIL) decision of 10 February 2022 represented by NOYB and Italy's supervisory authority (Garante) decision of 9 June 2022 regarding the complaint Google Analytics represented by NOYB, local case number 9782890.
[32] IP address truncation "IP address anonymisation" means that asterisks or zeros replace other digits in 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 (to the US).

of individuals' rights and freedoms, which gives Tele2 a special responsibility that entails high requirements for transfers to third countries, where IMY's overall assessment is that Tele2 has not demonstrated that it has carried out a sufficient analysis and mapping and has not taken the necessary security measures to limit the risks to data subjects.

At the same time, IMY recognises that there are factors that point in the opposite direction. IMY takes into account the specific situation following the judgment and the interpretation of the EDPB's recommendations, where there was a gap following the failure of the transfer tool to the US, as previously decided by the Commission, to be recognised by the CJEU. IMY also considers that Tele2 has taken some, albeit insufficient, measures to limit the personal data transferred by activating "anonymisation of IP addresses" through truncation.[33] Tele2 has analysed and mapped the life cycle of personal data in the Tool. This fact is also taken into account when assessing the gravity of the infringements.

Overall, IMY assesses, in light of the circumstances presented, that the infringements in question are of low severity. The starting point for the calculation of the penalty fee should therefore be set low in relation to the current maximum amount.

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

Based on an overall assessment of the aforementioned circumstances, the high turnover in relation to the observed infringements and in light of the fact that the administrative fine must be effective, proportionate and dissuasive, IMY assesses that the fine can be SEK 12,000,000 (twelve million).

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

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

Annex
Annex 1 - Information on the payment of a penalty payment

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

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 e-mail 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.