Integritetsskydds myndigheten

Coop Sverige AB
Englundavägen 4
17188 Solna

Document number:
DI-2020-11368

Date:
2023-06-30

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

Contents

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

Decision of the integrity protection authority

The Integritetsskyddsmyndigheten finds that Coop Sverige 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.coop.se, thereby transferring personal data to third countries without complying with the conditions laid down in Chapter V of the GDPR.

The Integritetsskyddsmyndigheten orders Coop Sverige Aktiebolag on the basis of Art. 58(2)(d) of the GDPR to ensure that its processing of personal data in the context of Coop Sverige Aktiebolag's use of the Google Analytics tool complies with Article 44 and the other provisions of Chapter V. In particular, Coop Sverige Aktiebolag shall cease to use the version of the Google Analytics tool used on 14 August 2020, unless adequate safeguards are in place. Those measures must be implemented no later than one month after the date on which this decision enters into force.

1 Description of the supervision case

1.1 The organisation

The Integritetsskyddsmyndigheten (IMY) has initiated supervision of Coop Sverige AB (hereinafter "Coop" 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 allegedly took place when the complainant visited the company's website, www.coop.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 procedure 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 Coop's website. During that 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 and also the Google New Order Data Processing Conditions for Google Advertising Products, Google processes personal data on behalf of the data controller (i.e. Google Analytics).

[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).

company) on behalf of the company. Google LLC is therefore to be classified as the Company's data processor under the aforementioned conditions.

During the complainant's visit to the company's website, Coop 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. In accordance with paragraph 10 of the terms and conditions on the processing of personal data for Google's advertising products, Coop 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.

1.3 What Coop has stated

Coop Sverige AB has essentially stated the following.

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

Coop 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 not established in any Member State other than Sweden and has not taken such a decision for any other European website.

The purpose of Coop's use of the Tool is to fulfil the purpose of developing and improving Coop's operations, products and services. For example, the Tool is used to analyse and evaluate (i) how data subjects use coop.se, (ii) Coop's customer personalisation on coop.se and (iii) Coop's advertising campaigns. Based on the insights provided by the Tool, Coop may decide on measures to improve and optimise Coop's products, services (e.g. features offered on coop.se and their placement or personalisation on coop.se) and marketing or decide to develop new products or services. For this purpose, it is necessary to retain relevant unique identifiers for the analyses performed in order to create reliable and verifiable results.

The tool is used to create analyses and reports that facilitate decision-making linked to the purposes of 1) providing a personalised experience in Coop's digital channels and 2) marketing and communication in Coop's and third party digital channels.

[2] CJEU judgment Facebook Ireland and Schrems (Schrems II), C-311/18, EU:C:2020:559.

The purpose of the Tool can also be fulfilled with the implementation of a server side container, which means that the visitor's IP address will not be sent to the Tool (see below). Coop does not need IP addresses as identifiers to fulfil the purpose of the Tool. The purpose of the Tool is to create reports for decision-making for the purpose of *developing and improving Coop's operations, products and services*. Examples of information needed in these reports. Could be the exposures that lead to a purchase in order to evaluate their effectiveness, e.g. product displays, prescription displays or campaigns. In this context, it is therefore the measurement, not the IP address, that determines whether the purpose of the Tool can be fulfilled.

Coop's customers are on the Swedish market and Coop targets only the Swedish market. However, for practical reasons and the prohibition of discrimination against consumers, and in some cases traders, under the Geoblocking Regulation[3] , there is no restriction on who can visit Coop's website. Coop does not specifically analyse from which countries traffic to the website comes.

1.3.2 Recipients of the data

In the context of Coop's use of the Tool on the Website, personal data is disclosed to a number of entities, all of which are processors or sub-processors of Coop, 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 the use of the Tool on the Website, Coop and its data processors (the Recipients) process the data listed below.

1. User behaviour on the website based on values submitted via variables on the website (e.g. filterCombination, Page title, Referrer or storeName).
2. Device information (e.g. flashVersion, javaEnabled, language or screen colour choice).
3. Customer status (i.e. whether the user visits the Coop website in logged-in or logged-out mode or as a business customer).
4. Online identifiers (e.g. IP address, userID, transactionID, clientID, gclid, dclid or Device ID).
5. Transaction data based on values submitted via variables on the website (such as numberCup, Transaction - dimension50 (boughtRecipe), Transaction - dimension7 (deliveryMethod), orderID or deliveryTime).

1.3.4 Categories of persons concerned by the processing

The categories of persons concerned by the processing are visitors, private customers (non-member with account), business customers and members of Coop Member.

The tool is not set up and is not used to process special categories of personal data or personal data of particularly vulnerable persons.

[3] Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on measures against unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment in the internal market.

1.3.5 When the code of the Tool is executed and Recipients are granted access
Once a user has made their consent choices, the user's personal data, to varying degrees, will be sent to the Tool. The content is integrated and executed after the conditions in Coop's consent manager are met.

1.3.6 How long the personal data processed is stored
The personal data processed in the Tool is stored for a maximum of 38 months and then deleted.

1.3.7 Which countries the personal data is processed in
The personal data is processed, among others, in the USA.

1.3.8 Coop's relationship with Google LCC
Coop purchases the licence for the Tool through a reseller who is Coop's data processor. Coop and the data processor have entered into a data processor agreement that regulates the setup and administration of the Tool. The data processor in turn independently administers all activities in relation to Google. For example, the data processor manages the entire set-up of the Tool, remuneration for the service and contacts with Google regarding support.
In other words, Google is acting exclusively on the instructions of Coop's data processor.

Google also applies contractual terms and conditions between itself and the retailer that regulate Google's processing of personal data as a processor in relation to the retailer, whereby the retailer is Coop's processor. Google thereby becomes Coop's sub-processor. This view of the division of roles is consistent with the view of Coop's data processor and Google. In addition, the settings enabling the use of personal data in the Tool for Google's own purposes are disabled.

In light of (i) the fact that Coop's data processor acts in accordance with Coop's instructions, (ii) the structure of the agreement and how the parties involved view the division of roles, and (iii) the fact that data sharing for Google's own purposes is deactivated, Coop's assessment is that Google is a sub-processor to Coop in relation to personal data processing in the Tool.

1.3.9 Ensuring that the processing does not take place for the Recipients' own purposes Coop discloses the personal data to its processors. Coop has entered into data processing agreements with these processors. The agreements contain points relating to Coop's right to audit/audit through which Coop can verify that the processor does not process personal data for its own purposes or for the purposes of third parties.

As part of its work with the General Data Protection Regulation, Coop applies a procedure to ensure compliance. The procedure includes an annual wheel whose purpose is to ensure good compliance over time. The annual cycle is divided into four parts, where the follow-up of counselling relationships is included in the third part. Within the framework of the follow-up work according to the annual wheel, it is possible to ensure that data processors only process personal data on behalf of Coop.

In connection with the implementation of the consent manager, additional measures have also been taken to ensure that Coop does not allow Recipients to process personal data of Coop's visitors, customers and members for the purpose of

their own purposes. There are procedures in place that state that each responsible employee must ensure that no sharing of personal data takes place through in-service solutions.

1.3.10 Description of Coop's use of the Tool

Coop sends various identifiers via the measurement set up on its website. Common to all identifiers is that they are unique to the data subjects' interactions related to the website www.coop.se. In other words, a data subject is not assigned a single identifier that applies to websites other than Coop's website.

The example below describes a report where Coop wants to understand which products are popular to buy online and how these have been exposed to the customer on the Coop website. When the customer makes their purchase in the Coop's e-commerce, the following information is sent to the Tool (in the form of a variable, description and example of value):

- Id - Product ID - 3600542020855
- Variant - Size of the package (e.g. 200 g etc.) - undefined
- Price - Price of the product - 26.5
- List - The products on the site are presented in a product list that can have different names, e.g. product search, site search, search dropdown - product search.
- listPosition - The position of the list among other product lists (from 0 onwards) - 0
- position - The position of the product in the product list (from 0 upwards) - 0
- name - Product name - Balsam Goodbye Damage
- brand - Trade mark - Fructis
- category - Product category area - Beauty & Hygiene -Hair care -

Conditioner The identifiers transmitted are the following:

1. *clientID* - used to determine whether a registrant is new or returning. New clientIDs are generated if a registrant clears their cookies and re-enters the site.
2. *userID* - generated for registrants with a login account on coop.se and used to determine whether a registrant has a login account or not.
3. *gclid and dclid* - generated for each unique ad click. The purpose is to be able to attribute a click to a specific advert, for example to get aggregated information on how many times the advert has been shown or how many people have interacted with it.
4. *transactionID* - generated in connection with a purchase on coop.se and corresponds to an order number.

Based on the information stated above, Coop can, among other things, draw conclusions about popular products that lead to purchases, how the customer journey started and the type of registrant who made the purchase (e.g. new or returning member/customer or member/customer with a login account). These conclusions are not dependent on data subjects' public IP addresses being sent to the Tool and therefore the purpose can be fulfilled regardless of whether public IP addresses are sent or not.

In light of the implementation of the server side container, Coop also wishes to clarify that data subjects' IP addresses are only processed through the following processing operations: 1) collection on the company's website, 2) transfer to the server side container and 3) conversion of the unique IP addresses into a generic IP address for

server side container. Collection, transmission and conversion are real-time and no public IP addresses are stored.

1.3.11 Own checks on transfers affected by the Schrems II judgement
In light of the Schrems II judgement, Coop has carried out a review of its third country transfers. In the autumn of 2021, Coop has also carried out an audit of the Tool where Coop has been able to establish that international data transfers take place through the use of the Tool. As part of this work, ongoing measures have been taken to further increase privacy protection related to the data subjects whose personal data is affected.

1.3.12 Transfer tools according to Chapter V of the General Data Protection Regulation Transfers to third countries take place on the basis of the European Commission's standard contractual clauses (data processors), which are incorporated in the agreement concluded between Google and Coop's data processor. According to the agreement, Coop's processor is the exporter of the personal data to the Tool.

Coop bases the data transfers to the US on the standard contractual clauses for the transfer of personal data to processors in third countries.
The standard contractual clauses in this case were concluded between Google LLC and its processor. In this context, it should be noted that Google provides standardised services and does not offer its customers the possibility of negotiating the terms and conditions of its services. Since those terms are not subject to negotiation, there are no signed copies available; instead, Coop has attached the data processing terms in which the standard contractual clauses have been incorporated and which apply in accordance with the contract concluded by its processor.

Coop is taking steps to ensure that the existing standard contractual clauses are always updated according to the latest version of the European Commission's standard contractual clauses.

1.3.13 Verification of obstacles to enforcement in third country legislation
Checking for obstacles in third country legislation is part of Coop's efforts to review its third country transfers. However, Coop has noted the criticism levelled by the European Court of Justice against US legislation and takes this into account in the choice of complementary safeguards.

1.3.14 Additional safeguards taken in addition to those taken by Google
Implementation of additional safeguards is part of Coop's efforts to review its third country transfers. According to information provided by Google, several security measures are provided that Google considers to be such additional safeguards that can be implemented together with the standard contractual clauses.

Coop has also carried out work to set up a server side container, in order to increase control over the way in which data is sent to the Tool.

Coop considers that Google's contractual and organisational measures can be considered to minimise the actual risk of the disclosure of personal data to third countries ultimately taking place. However, Google's Transparency Report, Global requests for user information, shows that Google regularly receives enquiries from US authorities about what applies when accessing personal data stored by Google. Coop's assessment is that the real risk of data being disclosed to US intelligence services is small. However, it cannot be eliminated by any measures taken by either Google or Coop.

Furthermore, Coop considers that the additional measures taken to minimise the possibility of surveillance also reinforce the rights and freedoms of Coop's customers, as they cannot be identified through the data transferred.

In summary, through these measures, only one and the same generic IP address is transferred to the Tool, regardless of the data subject's unique IP address. Coop has also activated the function in the Tool for so-called IP anonymisation, but in light of the server side container, this measure is, according to the company, superfluous.

1.3.14.1 General about server side container

A server side container is generally implemented to either improve 1) website performance or 2) security. In terms of performance, fewer tags can be used related to the measurement set up on the Website, which means less code on the client side and, for example, the Website can be loaded faster.

In terms of security, visitors' data can be better protected and the site owner retains greater control over data collected and distributed in an environment controlled by the site owner. When data is first sent to a cloud-based solution, it can be processed and redistributed with tags that the site owner controls.

1.3.14.2 Coop's implementation of server side container

The purpose of the server side container that Coop has implemented is to improve the security of the data sent. More specifically, the purpose is to be able to protect the data subjects' personal integrity in a good and secure way. The server side container acts as a proxy between the data subject's browser and the Tool where Coop has chosen to implement the server side container in a way that ensures that the data subject's browser's public IP address is never transferred to the Tool.

Implementation can be described as follows. A data subject visits the website www.coop.se in their browser. The Google Analytics script is downloaded from the server side container instead of being downloaded directly from the Google Analytics servers. This results in the transfer of the data subject's IP address as well as information on user behaviour, device information, customer status, online identifiers and transaction data (as per points 1-5 above under section 1.3.10) to the server side container, instead of directly to Google Analytics. Once the Google Analytics script has been downloaded from the server side container, a new call is made from the server side container to the Google Analytics servers. Since the call is made from the server side container, there is no transfer of the data subject's public IP address to Google Analytics. Coop has configured the server side container in such a way that all data as described above, except for the data subject's public IP address, passes through the server side container to Google Analytics. Google Analytics receives the data sent from the server side container and the data (information) sent is populated in reports through the measurement set up on the website www.coop.se.

The processing involved in the above - i.e. receiving, converting and forwarding the call - takes place in the working memory of the server side container. This means that all processing takes place in real time and no data is permanently stored. In other words, registrants' public IP addresses are not stored in the server-side container, nor are they exposed to Google Analytics servers. In addition, all communication from the browser, via the server side container, to the Tool is encrypted.

This process cannot be reversed as the information is not stored and the conversion is not based on a one-to-one relationship allowing the use of a "key" to recreate the public IP addresses.

Coop has activated Google's IP anonymisation feature. This means that the IP address sent to the Tool is truncated. This is done by Google removing part of the IP address before the IP address is stored on disc. For an IPv4 address, the last octet of the address is replaced with a zero. For an IPv6 address, the last 80 bits are replaced with zeros. The action cannot be reversed, but since this action is done by Google in the Tool, Coop has also chosen to implement a server side container.

In the case of Coop, the IP anonymisation feature is enabled and applied to the generic IP address sent via the server side container. However, in this context, the feature is redundant given that the server side container prevents data subjects' public IP addresses from being sent to the Tool. Coop's assessment is that the server side container as a measure is a sufficient protection measure, but that it does not hurt to also have the IP anonymisation function activated in 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.
Coop has been given the opportunity to comment on Google LLC's opinion. Google LLC'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. 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.

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 function, 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 known as 'data at rest' in data centres, where user data is stored on a disk or backup media to prevent unauthorised access to the data.

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

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

2. Justification of the decision

2.1 The framework of the audit

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

2.2 It is a matter of processing personal data

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

According to Article 1(2), the GDPR aims to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data. According to Article 4(1) of the Regulation, personal data are "*any information relating to an identified or identifiable natural person ('data subject'), an identifiable natural person being one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or online identifiers, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*". To determine whether a natural person is identifiable, account should be taken of any means likely to be used, either by the controller or by another person, to directly or indirectly identify the natural person (Recital 26 of the GDPR).

The concept of personal data can include any information, whether objective or subjective, provided that it "relates" to a specific person, which it does if it is linked to that person by virtue of its content, purpose or effect.[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', 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 are reasonably *likely to be used to* identify the natural person, all objective factors, such as the cost and time required for identification, taking into account both the technology available at the time of the processing, should be taken into account. Article 4(5) of the Regulation states that '*pseudonymisation' means the* processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of supplementary information, provided that such supplementary information is kept separately and is subject to technical and organisational measures ensuring that the personal data are not attributed to an identified or identifiable natural person.

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

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

[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.

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 the Breyer judgment, the CJEU has recognised that dynamic IP addresses constitute personal data in relation to the data controller, where the latter also has the legal possibility of identifying the holders of the internet connections by means of the additional information available to third parties.[7]

2.2.2 The assessment of the Data Protection Authority

To determine whether the data processed through the Tool constitutes personal data, IMY will consider whether Google or Coop, through the implementation of the Tool, can identify individuals, such as complainants, 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 Coop 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 transmitted 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 Coop (i.e. the company's account ID for Google Analytics).
2. Web address (URL) and HTML title of the website and webpage 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 generic IP address created by Coop's implementation of a server side container.

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 render individuals identifiable, it must nevertheless be taken into account that in the present case those unique identifiers can be combined with additional elements (as referred to in paragraphs 2 to 4 above) and that it is possible to draw conclusions in relation to information (as referred to in paragraphs

[6] ECJ judgment Breyer, C-582/14, EU:C:2016:779, paragraphs 45-46.

[7] 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.

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

2-4 above) that result in data being personal data, even if 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 Coop 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 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 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 (according to points 1-3 above) with which the IP address can be combined to enable identification. Coop's measure regarding the generic IP address created by Coop's implementation of a server side container prevents the transfer of the IP address to third countries, but still enables identification at Coop, which in itself is sufficient for the data to constitute personal data.

[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.

IMY notes that there may also be reasons to compare IP addresses (even generic ones) 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 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.[10]

In addition, the complainant's personal data were processed on 14 August 2020, as the complainant was logged in to his Google account when visiting the Website, thereby enabling conclusions to be drawn about the individual based on his registration with Google. It follows from Google's statement that the implementation of the Tool on a website makes it possible to obtain information that a user of a Google account (i.e. a 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 generic IP addresses and the possibility of combining these with additional data, Coop's use of the Tool on a website involves the processing of personal data.

2.3 Coop is the data controller for the processing

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

The answers provided by Coop show that the company has made the decision to implement the Tool on the Website. Furthermore, it appears that Coop's purpose with this 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, Coop has established the purposes and means of the collection and the

[10] 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 subsequent transfer of these personal data. Coop 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 Coop's transfer of personal data to the United States is compatible with Article 44 of the GDPR and is supported by a Chapter V transfer tool.

2.4.1 Applicable provisions, etc.

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

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

In Schrems II, the CJEU annulled the previous adequacy decision for the US.[11] 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 may be able to guarantee the necessary protection of data solely on the basis of the standard data protection clauses, there are other situations in which the provisions of those clauses cannot be a sufficient means of ensuring in practice effective protection of the personal data transferred to the third country concerned."* According to the CJEU, this is *"inter alia*

[11] 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 European Union-US Privacy Shield.

the case where the law of that third country authorises the authorities of that third country to interfere with the rights of the data subjects in relation to those data."[12]

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 standard 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".*[13]*

The recommendations of the European Data Protection Board (EDPB) on the consequences of the judgement[14] 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"*.[15]

The EDPB recommendations indicate that such additional safeguards can be divided into three categories: contractual, organisational and technical.[16]

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 [...]".[17]*

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*

---

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

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*".[19] 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 which may include, inter alia, network identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts*".[20]

2.4.2 Assessment of the Data Protection Authority

2.4.2.1 Applicable transfer tool

The investigation shows that Coop 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 Decision of 4 June 2021 (2021/914/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.

However, 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 the importer of the data into the United States, 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.

---

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

In Schrems II, the CJEU held that the US surveillance programmes based on 702 FISA, Executive Order 12333 ('E.O. 12333') and Presidential Policy Directive 28 ('PPD-28') of the US legislation do not meet the minimum requirements of EU law under the principle of proportionality. This means that the monitoring programmes based on those provisions cannot be considered to be limited to what is strictly necessary. Moreover, the Court found that the surveillance programmes do not provide data subjects with rights that can be enforced against the US authorities in court, which means that those persons do not have the right to an effective remedy.[21]

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 Coop

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

As data controller and exporter of the personal data, Coop is obliged to ensure compliance with the rules of the GDPR. This responsibility includes assessing, on a case-by-case basis, when transferring 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 (Coop) 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. Google has described these measures in its statement of 9 April 2021.

The question is whether the additional safeguards put in place by the company and Google LLC are effective, in other words, prevent US intelligence agencies from accessing the transferred personal data.

As regards the *contractual and organisational measures, it* can be noted that neither information to users of the Tool (such as Coop),[22] 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 unclear how Google LLC's '*careful scrutiny of each request*' for the 'lawfulness' of such requests is effective as an additional safeguard, given that, according to the CJEU, even lawful legal requests from US intelligence agencies are not compatible with the requirements of EU data protection rules.

As regards the *technical measures* taken, neither Google LLC nor the company has clarified how the measures described - such as the protection of communications between Google services, the protection of data during transfer between data centres, the 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.

---

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

In the case of encryption technologies - such as 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 transfer imported personal data in its possession, including any encryption keys required to make the data intelligible.[23] 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 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 makes individuals identifiable as described above.

With regard to Google's 'IP address anonymisation' measure in the form of truncation[24], 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 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.

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 Coop's own additional safeguards

Coop has stated that it has taken additional protective measures beyond those taken by Google (truncation[25] of the last octet when measured data is transmitted).
According to the company, these consist of a 'server side container', set up in order to increase control over the way in which data is sent to the Tool, which means that only a single generic IP address is transferred to the Tool, regardless of the data subject's unique IP address.

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

IMY notes that Coop also transfers a number of other unique identifiers (clientID, userID, gclid and dclid and transactionID),[26] the purpose of which is to be able to distinguish the complainant at Google. The server side container means that, after the IP address collected by Coop (but before the transfer to Google), the IP number is replaced by a generic IP number that is the same for all visitors to Coop's website.

The

[23] See EDPB Recommendations 01/2020, paragraph 81.
[24] 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).
[25] 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 can still be distinguished from the other IP addresses (255 options), as the IP address can be linked to other data transmitted (e.g. device and time of visit) to third countries. Last octet masking (Google's measure) is not an additional privacy enhancing measure than server side container, as this measure only masks the last octet of an already anonymised IP address.

The unique identifiers (clientID, userID, gclid and dclid and transactionID) are also transmitted via the server side container (and the IP anonymisation), but are transmitted in an unaltered form, i.e. in plain text, which means that this data is distinguishable and thus linkable. IMY concludes that since the data transmitted can be linked to other data also transmitted to Google LLC, the additional safeguards are not sufficient.

Instead, in order to ensure effective safeguards, all unique identifiers should be transmitted in an altered form (i.e. not in plain text) that makes the transmitted data unlinkable.

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*

In light of the above, IMY finds that Coop has not demonstrated that any of the tools listed in Chapter V of the GDPR can be used to transfer personal data of visitors to its website - in particular unique identifiers, IP addresses, browser data and metadata - to Google LLC in the United States.

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

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

3 Choice of intervention

3.1 Legal regulation

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

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.

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 found above that the transfers of personal data to the US via the Google Analytics tool, for which Coop is responsible, are in breach of Article 44 of the GDPR. As stated above, breaches of that provision may give rise to penalties. In this case, it is a question of a serious infringement that should normally lead to a penalty payment.

In assessing whether a penalty should be imposed in this case, the fact that the infringement has taken place by Coop 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 was 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[27], 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.

In *mitigation,* the specific situation following the judgment and the interpretation of the EDPB's recommendations should be taken into account, where there was a gap after the transfer tool to the US was rejected by the CJEU in the Commission's previous decision. It should also be noted that the investigation shows that Coop has analysed the life cycle of personal data in the Tool. Coop has also taken measures such as a so-called server side container, which was set up in order to increase control over the way in which data is sent to the Tool and which means that only one and the same generic IP address is transferred to the Tool, regardless of the data subject's unique IP address. The company has also activated Google's measure 'anonymisation of IP addresses' through truncation. Coop has thus taken extensive technical measures to try to limit the risks to data subjects and to cure the deficiencies. In so doing, Coop has also believed that it has succeeded, even though those measures have now been shown not to be sufficiently effective to prevent US intelligence services from accessing the data or to render such access ineffective.

In an overall assessment, IMY finds that there is reason in this case to refrain from imposing an administrative fine on Coop 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 the transfer of personal data invoked by Coop 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, Coop must be ordered, pursuant to Article 58(2)(d) of the GDPR, to ensure that the company's processing of

[27] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 under 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.

personal data in the context of the use of the Google Analytics tool shall comply with Article 44 and the other provisions of Chapter V. In particular, Coop shall cease using the version of the Google Analytics tool used on 14 August 2020, unless adequate safeguards are in place. Those measures shall be implemented no later than one month after the date of entry into force of this Decision.

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

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