Beet AB

Box 7140
103 87 Stockholm

Org.nr: 556911-3789
www.beet.se

4 JULY, 2023 – UPDATED 17 JULY 2023

Information and Recommendations related to IMY:s decision on Google Analytics 3/7-2023 & EC:s decision on DPF 10/7-2023

Tomas
Lindqvist

Channel Lead – Analytics & Measurement

Content

1. What has happened & background
2. Key facts that are good to know
3. Current recommendations
4. Summary
5. What should we as a company do now?
6. Disclosure
7. Term and function explanations
8. Update Log

1. What has happened & background

IMY (Integritetsskyddsmyndigheten - Integrity Protection Authority) issued a statement and decision on July 3rd, similar to previous authorities in Denmark, France, Italy, Austria, and Norway"s preliminary statement. The main difference in the Swedish decision is that it is the first decision where sanction fines have been imposed. Otherwise, the decisions are largely similar in terms of the grounds on which they were made.

In summary, the decision states that the standard use of Google Analytics (Universal Analytics - UA) is not compatible with GDPR. The four companies involved (Tele2, CDON, DI, and Coop) have not implemented sufficient technical measures in their use of UA to ensure an equivalent level of data protection for data transferred to the United States, as is guaranteed within the EU under the GDPR law.

The case stems from a complaint filed by the interest organization NOYB (None of Your Business) against 101 EU-companies (in Sweden, four for Google Analytics and two for Facebook). Sweden is the fifth country to make an official decision regarding the complaints. NOYB filed these complaints in connection with, and shortly after, the Schrems II-decision in July 2020 (also driven by NOYB).

In essence, the Schrems II-decision concluded that the Standard Contractual Clauses (SCCs) that Google and other companies rely on for their usage do not provide sufficient protection on their own, and additional measures need to be taken. The ruling stated that the companies had not implemented adequate measures.

The decision from IMY is thus made in the same manner as the previous countries but is the first to decide on sanction fines.

Unfortunately, IMY:s decisions provide limited information about what exactly is deemed "insufficient action" from a technical perspective in the investigations. We are actively working to compile and update both information and recommendations based on our best knowledge. As a result, this document may be updated with new information and recommendations in the future.

Update 6/7/2023: IMY changes the title of the press release from "Companies must stop using Google Analytics" to "Four companies must stop using Google Analytics". This does not change the implication that action needs to be taken, but it clarifies that the decision applies specifically to these four companies now.

Update 17/7-2023:

On July 10th 2023, the European Commission (EC) adopted an adequacy decision regarding the new Data Protection Framework (DPF), replacing the Privacy Shield, concerning secure and reliable data transfers between the EU and the USA.

The use of the new framework as support for data transfers between the EU and the USA has been approved as of July 10th, 2023, for certified businesses.

A website and information about the certified entities have been released on July 17th 2023, where you can see which businesses are certified. Therefore, it was only on the 17th that we were able to know which entities are actually approved, even though the decision took effect immediately on July 10th, in order to compile our recommendations in connection with the decision.

IMY (Integritetsskyddsmyndigheten) has also released a press release regarding the EC:s adequacy decision for the DPF: https://www.imy.se/nyheter/eu/

What does the EC's 'adequacy' decision mean?
In practice, it means that the use of tools from certified partners is now allowed for the transfer of personal data. Essentially, if a transfer made within the EU is approved, it would now also be approved for transfers from the EU to the USA and vice versa, for transfers that are approved within the USA.

Link to the decision:
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

Which businesses are now certified?
For a complete list, please refer to the official website. However, it can be mentioned directly that Google, which was affected by IMY's decision regarding Google Analytics, is certified under the DPF, along with Meta, Microsoft, and many others.

Therefore, the use of Google Analytics (UA & GA4) is now allowed under the DPF.

Please note that it is still important to follow GDPR guidelines on data minimization, obfuscation, and limitation of data retention, regardless of how and where the collection is done and the data is sent.

Link to DPF-certified entities: https://www.dataprivacyframework.gov/s/participant-search

What about our recommendations in sections 3 and 4?

Although our recommendations were made in a context without the DPF, they are still relevant in a situation where the DPF would be invalidated, in a 'Schrems-III' scenario, similar to how the Privacy Shield was invalidated by Schrems-II (NOYB has already officially announced that they will challenge the adequacy decision for the DPF, and we can expect legal proceedings to commence in early 2024).

Thus, there is a risk that a similar situation may arise as the three years between Schrems-II and the adequacy of DPF following a potential Schrems-III decision, and our recommendations still serve as guidance for the potential risks they minimize if such a situation occurs.

We will continue to evaluate the risks and be available for technical advice regarding these issues for your specific situation upon request.

2. Key facts that are good to know

- The decision pertains to **UA**, linked to a complaint from 2020 made in relation to Schrems II. Our assessment is that the **decision does not concern Google Analytics 4**.
  Please note that this assessment may change if we are provided with new knowledge.
- Tele2 currently uses GA4 through regular GTM implementation (Google Tag Manager). It is mentioned in the decision that Tele2 has disabled Google Analytics, which means it refers to UA (Universal Analytics).
- Google has been communicating the sunset (closure) of data processing in UA for over a year, with a milestone set for July 1, 2023. However, many accounts still have active data processing and are not "closed". Read more at: https://support.google.com/analytics/answer/11583528?hl=en
- DI and Coop have, from our understanding, implemented more extensive measures to achieve an equivalent level of protection with UA (although they also received the same verdict), but they have not incurred any penalty sanction fines.

IMPORTANT! It is important to note that UA is not considered uninstalled just because "new data" is no longer processed in that specific account/property. **Uninstalling the scripts from the site or Google Tag Manager** that sends the data is necessary to stop sending data to Google/USA, as processing into your account might be stopped by Google even if they are receiving the data.

3. Current recommendations

These recommendations may be subject to change and are based on our best interpretation of the information we have at the moment.

1. Clear "stop now" regarding the use of UA based on IMY decisions

The decisions have made it clear that the use of UA"s IP anonymization function (*see section 7) is not sufficient. Coop and Dagens Industri, both of which received milder judgments, implemented a proxy to completely remove IP addresses before sending data to Google, which is a more robust technical measure.

1.1. <u>Stop sending visitors" IP addresses to Google when using UA</u>

Option 1: Completely uninstall UA implementations from GTM/Site and stop sending any data to UA.
(UA:s data handling should have been shut down by Google on July 1st anyway, although it currently appears to continue for many implementations that Beet is monitoring).
Option 2: Ensure that IP addresses cannot be sent to Google/USA when using UA.

1.1.1. For implementations directly on-site and through GTM, switch to server-side implementation and enable IP removal (requires setting up a GTM-server).

1.1.2. For server-side implementations, enable IP removal if it is not already activated.
Note: Removing the IP address will result in the loss of all GEO-IP-data, and no location data will be available.

1.2. <u>Do not submit/stop submitting personal information or data that can be easily linked to personal information</u>

Unfortunately, the IMY-decisions do not clearly specify what constitutes personal information beyond IP addresses. Therefore, it is recommended to apply the precautionary principle by minimizing and abstracting data to minimize the risk.

2. Precautionary measures for UA and GA4 based on IMY decisions

The measures are grouped according to the level of risk we believe would be mitigated by implementing the measure. “High Risk” can be seen as measures to minimize what we perceive as the greatest risks, and so on.

2.1. Precautionary measures for the use of Universal Analytics:

These below measures aim to minimize the risk of the data collected/collected for UA being classified as "personal information" in specific usage scenarios by isolating the data to its UA-account.

High risk:

- Disable/do not use "Google Signals"

According to our interpretation of the decisions, this appears to be the greatest risk exposure, in addition to points 1.1 and 1.2, as Google knows the users through Google accounts. Part of that data is shared with the UA-account based on the data provided to Google, which can potentially classify the data set as personal information, even if not all data is received from Google.

Medium risk:

- Disable/do not use "Advanced Settings to Allow for Ads Personalization"

See point 2.2. “Low Risk” point bellow regarding same feature of GA4 and what consequences of disabling it are.

Low risk:

- Do not share/stop sharing "Audiences and Conversions" with Google Ads.

2.2. Precautionary measures for the use of GA4:

(not part of the current IMY decisions, but similar features available as in UA)

High Risk

- Disable/do not use "Google Signals" (see 2.2.a.)

Medium Risk

- Implement GTM Server as a data gateway for GA4 before sending data to Google/USA, and thereby filter out IP addresses in your owned environments

GA4 has a technical difference compared to UA where data first goes to an EU-based data center before being sent to the USA (and thus becoming a data transfer to the USA). In this intermediate step, they remove the IP addresses, which are not forwarded. Therefore, GA4 is more secure and does not expose IP addresses in the same way as UA. However, one would however need to take Google at their word that they actually does this, and it is also something one cannot prove in case of an audit. Therefore, we consider it a medium-risk to do a regular implementation in GA4 and instead recommend implementing through a GTM server (a data gateway that you own).

- Disable/do not use "Granular location and device data collection" within the EU. Turn it off for all countries within the EU (** See Section 7)

This feature increases the amount of detailed data related to a user"s device and location that is stored and linked to the visitor"s data set. The risk here is mainly associated with having too many different data points within the same visit, which increases the risk of identification possibilities, thus going against the GDPR directive regarding minimizing data collection unless strictly necessary.

Låg risk

- Disable/do not use "Advanced Settings to Allow for Ads Personalization" within the EU (turn it off for all countries within the EU) and thus do not share/stop sharing "Audiences" or "Conversions" with Google Ads.

This feature controls which data can be forwarded to Google Ads and used for advertising related to the approved regions. Disabling this feature can have a significant impact on one"s Google Ads marketing if these functions are currently used and should be taken into consideration. The feature itself determines what is allowed to be done with the data after it has been transferred, and we assess that the risk associated with the data transfer itself is low.

- Implement data hashing/extra pseudonymization of various potential identifiers such as cookie IDs, transaction IDs, etc.

3. Alternative platforms to consider for the future

Note that none of these are fully comparable direct replacements for UA/GA4, but they are GDPR-compliant alternatives that we can assist with based on our expertise:

- **PiwikPro** (an alternative for e-commerce and lead sites, similar to UA)

- **Matomo** (open-source and built similar to UA, suitable for lead sites but has a limited e-commerce module)

- **Evaluation of other alternatives** (there are more tools out there and new ones emerging, where we can provide our expertise for evaluation and assistance)

4. Summary

Update 17/7-2023: See details on how the EC's adequacy decision for the DPF on 10/7-2023 affects everything in general under the "What has happened & background" section.

The decision is in line with other countries" authorities, although sanction fines have been imposed. The clearest violation they focus on is the sharing of IP addresses with Google. However, for other areas it is not entirely clear what grounds the decision is based on, but there are indications that data sharing with Google, such as Google Signals, could classify the data set as personal information and potentially enable other uses.

Our recommendations provided focus on:

- **Eliminate risk -** *completely disabling UA and switching to approved tools like PiwikPro & Matomo, or using GA4, which is not affected by the current issues and provides better protection than UA, although it is not currently certified as approved.*
- **Minimize risk -** *disabling features and implementing technical measures to minimize the risk in UA/GA4.*

A summary and risk assessment for features/data are currently as follows:
Direct risk: IP address and personal information
High risk: Google Signals and "potential" personal information
Medium risk: Other sharing features such as granular device/location data
Low risk: Non-obfuscated customer-IDs & user-IDs, aggregated data like audience lists (assuming consent mentions such potential use as audiences)
Very low risk: Pseudonymized-IDs, transaction-IDs, and similar data

5. What should we as a company do now?

Do not make hasty decisions. Yes, this is a serious situation and action/positioning will be required, but ensure that decisions are made based on informed choices.

1. Take a clear stance on our recommendations in point 1.1. and evaluate 1.2.
2. Conduct a risk assessment to determine where you want to position yourselves and what may be "business-critical" among the functions that we recommend potentially disabling under Section 2.
3. If further guidance is needed regarding our recommendations, provide feedback with your questions, and we will help clarify and ensure that information and recommendations are understood correctly.
4. Potentially schedule a meeting to review our technical advice for your specific situation and establish a plan going forward.

6. Disclosure

This information is not intended to constitute legal advice. Root Digital Group and its subsidiaries, as well as employees, do not provide legal advice and therefore cannot be held responsible for direct or indirect losses arising from this information or due to inadequate or inaccurate information. For questions relating to GDPR and data management, Root Digital Group recommends consulting legal expertise.

7. Term and function explanations

* **IP anonymization** is the process of removing the last octet of an IP address, making 123.123.123.123 become 123.123.123.000. This anonymization is done by Google directly when the data reaches their systems. However, according to IMY, it is not considered sufficient protection, possibly because the data transfer has already occurred before anonymization takes place, and it may also be deemed tha the action is insufficient to no longer be considered personal information.

** Data points stored when using "**Granular location and device data collection**", which can be controlled for active and inactive regions:

GEO: City, Latitude (of city), Longitude (of city)

Device: Browser minor version, Browser User-Agent string, Device brand, Device model, Device name, Operating system minor version, Platform minor version, Screen resolution

8. Update Log

17/7-2023 - Added relevant information about the EC:s adequacy decision for the DPF under the "What has happened & background" section and included information on how our recommendations are interpreted in relation to it.

6/7-2023 - Linguistic adjustments and clarifications for improved readability and understanding

6/7/2023 - Added information about IMY:s title update for the press release under “What has happened & background” section. Additionally, changed “fine” to “sanction fine” for a more accurate description

6/7-2023 - Clarified information under the section “Key facts that may be good to know” for all the points and provided more details and references

5/7/2023 - Added sections “Disclosure” and “Term and Function Explanations” and expanded information about the IP address issue

5/7/2023 - Added a new “Low Risk” action under GA4 precautionary measures section “Implement data hashing/extra pseudonymization”

5/7/2023 - In the GA4 risk mitigation section, moved “Advanced Settings to Allow for Ads Personalization” from “Medium Risk” to “Low Risk” and combined it with the point “do not share/stop sharing “Audiences” or Conversions with Google Ads”

5/7/2023 - Added more contextual information to several actions under the precautionary measures for GA4 and in section 7

5/7/2023 - Expanded contextual explanation in the “Summary” section regarding the focus of recommendations

5/7/2023 - Added more information about the situation of DI and Coop under “Key Facts.

5/7/2023 - Added introductory thoughts “What should my company do now?” and clarified and separated point 3 into points 3 and 4