Complaint under GDPR and TTDSG

filed by
Kim Mustermensch, Musterstraße 123, 12345 Musterstadt, Musterland
(complainant, hereinafter: “I”)

against
the controller for the Android app “Sample App!”, assumed to be
Musterfirma, Musterstraße 123, 12345 Musterstadt, Musterland
(respondent, hereinafter: “the controller”)

on
March 15, 2024

regarding
Art. 6(1) GDPR (lawfulness of processing), Art. 25 GDPR (data protection by design and by default), Art. 5(1)(c) GDPR (data minimisation), § 25 TTDSG (privacy protection for terminal equipment)

under the reference
2024-abcdef
(please mention when replying)

1. Introduction

I am hereby filing a complaint under Art. 77(1) GDPR regarding the Android app "Sample App!" (hereinafter: "the app").

According to the Google Play Store page for the app[1], it is operated by Musterfirma, Musterstraße 123, 12345 Musterstadt, Musterland. I am thus assuming them to be the app's controller. Should this assumption be incorrect, my complaint is directed against the actual controller of the app.

I am a user of the app on my personal Android device. The Android device is only used by me personally. I have installed it through the Google Play Store. I am logged into the Google Play Store with my personal account.

My Android device has a SIM card installed that is registered to my name.

2. Facts

2.1. Preliminary remarks

To understand how the app is processing my data, I used the tools of the tweasel project[2], operated by Datenanfragen.de e. V., to perform an automated analysis of the app's network traffic. The analysis was performed on March 15, 2024 at 12:29:13 PM GMT+1 on version 0.32.3 of the app, downloaded from the Google Play Store, running on Android 13.

During this analysis, the app was run *without any user input* (i.e. there was no interaction with the app at all) and its network traffic was recorded. The recorded traffic was then analyzed for tracking and similar data transmissions. Based on that, the tweasel tools produced a technical report.

Both this technical report and the traffic recording are attached to this complaint as evidence. The report also contains a detailed description of the methodology used for the analysis and its basis in mobile privacy research.

Through the analysis, I unfortunately had to find out that the app performs tracking (as explained in Section 2.2) in violation of the GDPR and TTDSG (as explained in Section 4).

On March 15, 2024, I sent a notice to the controller making them aware of the violations I discovered and giving them the opportunity to remedy them.

In the interest of avoiding unnecessary work for the data protection authorities, the controller, and myself, I gave the controller a voluntary grace period of 60 days to bring their app in line with applicable data protection law. I also informed them that I planned on filing a complaint otherwise.

I have received a response from the controller in which they deny there being any violations in their app. I am providing an in-depth technical and legal argument as to why I do believe the controller is violating the GDPR and TTDSG in this complaint.

[1] https://play.google.com/store/apps/details?id=tld.sample.app
[2] https://docs.tweasel.org/

I am attaching my notice to the controller as well as any communication I have received from them in this matter to the complaint.

On March 15, 2024 at 12:29:13 PM GMT+1, and thus after the expiration of the voluntary grace period, I retested the app using the tweasel tools. Unfortunately, I had to find that the app still performs tracking in violation of the GDPR and TTDSG.

To verify that the tracking also affects me, I used the the "TrackerControl" app[3] on my personal Android device. This confirmed that the app also contacts those tracking servers on my own device.[4] I have attached the evidence for this in Appendix A1.

2.2. Tracking without interaction

In this section, I am detailing the tracking data transmissions that the app performed. I am only including transmissions from the second technical report from the tweasel project from March 15, 2024. All these transmissions thus occurred **at least 60 days after** I informed the controller of the violations I had initially discovered and gave them the opportunity to remedy them.

Additionally, I am only including transmissions to servers for which the log of the "TrackerControl" app confirmed that the app also contacts them on my personal device, as explained above. It is thus safe to assume that all these transmissions also affect me personally.

It further bears repeating that, as guaranteed by the analysis methodology, the tracking transmissions described here all occurred **without any interaction** with the app or any potential consent dialog.

2.3. BugSnag Session Tracking API

The app sent 1 request(s) to the tracker "BugSnag Session Tracking API", operated by "SmartBear Software".

BugSnag offers the following services:

- Error monitoring, collecting and visualizing crash data.[5]
- Real user monitoring, to "[o]ptimize your application based on real-time user actions with your application" and give "visibility into critical performance metrics like hot and cold app starts, network requests, screen-load time and more."[6]

---

[3] https://trackercontrol.org/#network-traffic-analysis

[4] Recording a phone's network traffic requires rooting the device and making severe configuration changes. Doing this is not feasible or advised for devices that are in actual day-to-day use. That is why the tweasel project provides public infrastructure for doing such testing on devices/emulators that are only used for this purpose. However, logging a list of DNS hostnames contacted by an app is possible without such severe procedures by installing the "TrackerControl" app.

While the results from this log don't allow for inspecting the actual data that was transmitted, they do prove that the app contacted the same tracking servers. In combination with the technical report by the tweasel project, for which the request content was actually analysed, this provides a very strong indication that I am affected by the same tracking. As I will elaborate on in Section 4.3, the controller has the burden of proving that their processing is in line with the GDPR. It would thus be on them to produce evidence for disproving the conclusion I am drawing here.

[5] https://www.bugsnag.com/error-monitoring/

[6] https://www.bugsnag.com/real-user-monitoring/

The Session Tracking API is used to "notify Bugsnag of sessions starting in web, mobile or desktop applications."[7]

Through these requests, at least the following information was transmitted:

Data type	Transmitted value(s)
Tracker SDK version	`5.28.4`
App version	`23.13.1, 26004526`
App ID	`com.airbnb.android`
Architecture	`x86_64`
OS name	`android`
OS version	`13`
Is device rooted?	`false`
Manufacturer	`Google`
Model	`sdk_gphone64_x86_64`
Language	`en_US`
Total RAM	`2061852672`
Other unique identifiers for the user, device, session, or installation	`ad2140b6-25f1-42d7-b45c-4c0e224ca64f, 7d5a6fd0d53a566b, ea5d71aa-0ecc-4d81-ac29-e7dedf9d0a43`
App start time	`2023-03-20T16:35:24.304Z`

The full content of this request and the method used for decoding the request and extracting this information is documented in the attached technical report.

2.4. Facebook Graph App Events API (query string)

The app sent 2 request(s) to the tracker "Facebook Graph App Events API (query string)", operated by "Facebook".

The Graph API is provided by Facebook to "get data into and out of the Facebook platform".[8] It can be accessed through the Facebook SDKs for Android[9] and iOS[10].

The App Events endpoint allows developers to "track actions that occur in [a] mobile app or web page such as app installs and purchase events" in order to "measure ad performance and build audiences for ad targeting". The Facebook SDK automatically logs app installs, app sessions, and in-app purchases using this endpoint. Additionally, developers can manually log their own events.[11]

Through these requests, at least the following information was transmitted:

Data type	Transmitted value(s)

[7] https://bugsnagsessiontrackingapi.docs.apiary.io/#reference/0/session/report-a-session-starting
[8] https://developers.facebook.com/docs/graph-api/overview
[9] https://developers.facebook.com/docs/android/graph
[10] https://developers.facebook.com/docs/ios/graph
[11] https://developers.facebook.com/docs/marketing-api/app-event-api

Device advertising ID (GAID/IDFA)	`1209d0b9-b959-42e6-b921-aa5d9d08c1af`
Other unique identifiers for the user, device, session, or installation	`XZ9dd82044-772f-4b99-b17b-208e9c3cc38b`
OS name	`android`
App ID	`com.airbnb.android`
App version	`26004526, 23.13.1`
OS version	`13`
Model	`sdk_gphone64_x86_64`
Language	`en_US`
Time zone	`GMT+01:00, Europe/Berlin`
Carrier	`T-Mobile`
Screen width	`1080`
Screen height	`2214`
Total disk space	`8`
Free disk space	`6`

The full content of this request and the method used for decoding the request and extracting this information is documented in the attached technical report.

2.5. Branch Attribution API

The app sent 3 request(s) to the tracker “Branch Attribution API”, operated by “Branch Metrics, Inc.”.

Branch offers the following services:

- Mobile attribution[12] to “[c]apture every customer touchpoint across any channel, platform, OS to optimize […] campaigns and maximize ROI.”[13]
- Ad conversion tracking. Branch can “[r]etarget app users who see a web ad and then purchase in the app, attribute revenue to the web ad that drove the install, and measure cumulative revenue from users across both web and app.”[14]
- Custom audiences to “communicate the perfect message to the ideal customer, at the right moment”. “Get higher return on ad spend (ROAS) with precision retargeting of high-value active users and eliminate wasted spend in your acquisition campaigns by excluding existing customers. Re-engage lapsed users, boost propensity to purchase, and increase sessions per user.”[15]
- Fraud protection.[16]

[12] https://www.branch.io/attribution/
[13] https://www.branch.io/features/
[14] https://www.branch.io/universal-ads/
[15] https://www.branch.io/engagement-builder/
[16] https://www.branch.io/fraud-protection/

Branch provides integrations to automatically "send Branch data to […] marketing and analytics partners to measure and optimize […] campaigns."[17]

The Branch Attribution API is used for "deep linking and session attribution. […] Every time the API is called, it will track an INSTALL, REINSTALL, or OPEN event in Branch and return deep link data in the response if the session is attributed."[18] It can also track "additional downstream conversion events" like PURCHASE.[19]

Through these requests, at least the following information was transmitted:

Data type	Transmitted value(s)
Device advertising ID (GAID/IDFA)	`1209d0b9-b959-42e6-b921-aa5d9d08c1af`
Other unique identifiers for the user, device, session, or installation	`048f96ec-220f-4860-95c4-62b2565dbbd3, 1172860168313205995, 1172860168363571074, 58efd809-326b-4bbd-b9ee-34900c536c89, c19d8fab-8e27-43e3-b854-e9a4c086c171`
Manufacturer	`Google`
Model	`sdk_gphone64_x86_64`
Screen width	`1080`
Screen height	`2214`
Network connection type	`wifi`
OS name	`Android`
OS version	`13, 33`
Language	`en, en_US`
Local IP address(es)	`10.0.0.1`
Architecture	`x86_64`
Carrier	`T-Mobile`
Country	`US`
App version	`23.13.1`
Tracker SDK version	`android5.0.3`

The full content of this request and the method used for decoding the request and extracting this information is documented in the attached technical report.

2.6. BugSnag Error Reporting API (Notify)

The app sent 1 request(s) to the tracker "BugSnag Error Reporting API (Notify)", operated by "SmartBear Software".

BugSnag offers the following services:

- Error monitoring, collecting and visualizing crash data.[20]

[17] https://www.branch.io/data-feeds/
[18] https://help.branch.io/developers-hub/reference/attribution-api
[19] https://help.branch.io/developers-hub/reference/attribution-api#tracking-downstream-events

- Real user monitoring, to "[o]ptimize your application based on real-time user actions with your application" and give "visibility into critical performance metrics like hot and cold app starts, network requests, screen-load time and more."[21]

The Error Reporting API is used to send error reports and crashes to BugSnag.[22]

Through these requests, at least the following information was transmitted:

Data type	**Transmitted value(s)**
Tracker SDK version	`5.28.4`
Other unique identifiers for the user, device, session, or installation	`7d5a6fd0d53a566b, ad2140b6-25f1-42d7-b45c-4c0e224ca64f, ea5d71aa-0ecc-4d81-ac29-e7dedf9d0a43`
App ID	`com.airbnb.android`
App version	`23.13.1, 26004526`
Time spent in app	`15275`
Is app in foreground?	`true`
Architecture	`x86_64`
Manufacturer	`Google, google`
Model	`sdk_gphone64_x86_64`
OS name	`android`
OS version	`13`
Free RAM	`1099014144`
Total RAM	`2061852672`
Is device rooted?	`false`
Orientation	`portrait`
Viewed page	`GPExploreMapFragment`
App start time	`2023-03-20T16:35:24.304Z`
App name	`Airbnb`
Is device an emulator?	`false`
Network connection type	`wifi`
Charging status	`false`
Screen height	`2214x1080`
Screen width	`2214x1080`
Battery level	`1`

The full content of this request and the method used for decoding the request and extracting this information is documented in the attached technical report.

[20] https://www.bugsnag.com/error-monitoring/
[21] https://www.bugsnag.com/real-user-monitoring/
[22] https://bugsnagerrorreportingapi.docs.apiary.io/#reference/0/minidump/send-error-reports

3. Context: Online tracking

The tracking practices employed in the app by the controller are part of a broader ecosystem of online tracking that has become pervasive across the web and mobile apps. Extensive research has again and again revealed ubiquitous violations of and a prevalent disregard for data protection law in this context. The vast amounts of personal data collected through such tracking activities are fed into an opaque and shadowy system consisting of thousands of companies, posing very real dangers to users.

3.1. Habitual violations of data protection law

Studies looking into tracking that happens without consent have proven how common tracking is, even before there was any user interaction at all.

On the web, research found between 49 % and 75 % of websites using tracking before the user interacted with a consent prompt or even after explicitly rejecting it.[23]

Studies analysing apps on Android and iOS found similar results, reporting around 75 % of apps contacting trackers without consent and between 55 % and 72 % of apps sharing unique device identifiers like the device ID.[24] In fact, apps transfer more personal data to trackers before obtaining consent than afterwards.[25] Developers are frequently not aware of their obligations under data protection law or misunderstand them.[26]

Websites and apps that do try to acquire users' consent, typically employ dark patterns and nudging to trick users into giving consent even if they don't actually want to do so. Multiple studies across the web and mobile found that around 90 % of consent dialogs employed at least one dark pattern that is explicitly explained to be infringing the GDPR's conditions for consent in publications by data protection authorities.[27] These dark patterns include making refusing consent harder than giving it, and overly highlighting the "accept" button compared to the "reject" button by color and/or size. It is important to note that all cited studies only observed a limited set of minimal conditions that are easy to evaluate automatically, meaning that the actual percentage of consent dialogs with violations is in all likelihood even higher.

---

[23] Trevisan/Traverso/Bassi/Mellia, 4 Years of EU Cookie Law: Results and Lessons Learned, 2019, https://petsymposium.org/popets/2019/popets-2019-0023.pdf; Papadogiannakis/Papadopoulos/Kourtellis/Markatos, User Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users, 2021, https://dl.acm.org/doi/10.1145/3442381.3450056

[24] Kollnig/Shuba/Binns/Van Kleek/Shadbolt, Are iPhones Really Better for Privacy? A Comparative Study of iOS and Android Apps, 2022, https://petsymposium.org/popets/2022/popets-2022-0033.pdf; Altpeter, Informed Consent? A Study of "Consent Dialogs" on Android and iOS, 2022, https://benjamin-altpeter.de/doc/thesis-consent-dialogs.pdf

[25] Koch/Altpeter/Johns, The OK Is Not Enough: A Large Scale Study of Consent Dialogs in Smartphone Applications, 2023, https://www.usenix.org/system/files/usenixsecurity23-koch.pdf; Altpeter, Informed Consent? A Study of "Consent Dialogs" on Android and iOS, 2022, https://benjamin-altpeter.de/doc/thesis-consent-dialogs.pdf

[26] Tin Nguyen/Backes/Marnau/Stock, Share First, Ask Later (or Never?) Studying Violations of GDPR's Explicit Consent in Android Apps, 2021, https://www.usenix.org/system/files/sec21-nguyen.pdf

[27] Koch/Altpeter/Johns, The OK Is Not Enough: A Large Scale Study of Consent Dialogs in Smartphone Applications, 2023, https://www.usenix.org/system/files/usenixsecurity23-koch.pdf; Altpeter, Informed Consent? A Study of "Consent Dialogs" on Android and iOS, 2022, https://benjamin-altpeter.de/doc/thesis-consent-dialogs.pdf; Nouwens/Liccardi/Veale/Karger/Kagal, Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, 2020, https://dl.acm.org/doi/10.1145/3313831.3376321

The dangers of such dark patterns and nudging are well established in relevant literature. Consent dialogs already do not work as a medium for conveying privacy-critical information to users, even when those users are concerned about their privacy and no dark patterns are used.[28] Experiments investigating the effect of various design variables in consent dialogs on user choices found that nudging, even in the form of seemingly small details, heavily increases consent rates.[29] For example, a highlighted "accept all" button results in significantly higher consent rates but at the same time users are not aware of its effects and regret their choice after being informed of those effects.[30]

Other research found websites registering supposed consent without user interaction or even after an explicit opt-out, as well as preselected options in half of consent dialogs.[31]

3.2. Real risks for data subjects

At the same time, these practices pose significant and very real risks to data subjects. Thousands of tracking companies worldwide constantly collect vast amounts of data on users on the web and on mobile and analyze intimate details about their lives. An analysis of self-declared privacy labels on Android found often downloaded apps, including apps explicitly aimed at children, admitting to collecting and sharing highly sensitive data like the user's sexual orientation or health information for tracking and advertising purposes.[32] Based on such data, they try to predict users' behaviours for example to target and influence users with ads and decide which products to display and at what price. They also claim to be able to assess companies' risks to protect against spam, compute credit scores, or prevent fraud.[33]

Additionally, trackers build profiles on users, categorizing them into segments, sometimes based on highly sensitive inferences like health conditions, religious beliefs, sexual orientation, income level, and more. To give just a few examples, reporting has found segments such as *heavy alcohol consumers*, *desire to lose weight*, *planning to adopt a child*, *diagnosis for leukemia*, *low income without perspective*, *conservative values*, and even *visits to sexual abuse treatment centers*. Trackers also score users on criteria like *often influenced by ads*, *inexperienced credit card users*, *lone wolves*, and *getting a raw deal out of life* to identify vulnerabilities.[34] Trackers conduct large-scale experiments, systematically optimizing how to persuade, manipulate, and trigger users.[35]

---

[28] Bauer/Bravo-Lillo/Fragkaki/Melicher, A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality, 2013, https://dl.acm.org/doi/10.1145/2517881.2517886

[29] Utz/Degeling/Fahl/Schaub/Holz, (Un)informed Consent: Studying GDPR Consent Notices in the Field, 2019, https://dl.acm.org/doi/10.1145/3319535.3354212; Nouwens/Liccardi/Veale/Karger/Kagal, Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, 2020, https://dl.acm.org/doi/10.1145/3313831.3376321

[30] Machuletz/Böhme, Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR, 2020, https://petsymposium.org/popets/2020/popets-2020-0037.pdf

[31] Matte/Bielova/Santos, Do Cookie Banners Respect my Choice?: Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework, 2020, https://ieeexplore.ieee.org/document/9152617

[32] Altpeter, Worrying confessions: A look at data safety labels on Android, 2022, https://www.datarequests.org/blog/android-data-safety-labels-analysis/

[33] Sieben in Altpeter/Sieben, Tracking und Datenschutzrechte, 2023, https://static.dacdn.de/talks/slides/2023-09-08-topio.pdf, slide 75

[34] Keegan/Eastwood, From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You, 2023, https://themarkup.org/privacy/2023/06/08/from-heavy-

Crucially, trackers don't need to know users' legal identities for any of this profiling. They collect and assign unique identifiers to track users, and share and link IDs among each other in order to more precisely follow users across websites and apps.[36] For trackers, these IDs are often even more useful than legal names. After all, names are not unique whereas IDs are specifically designed to precisely identify a single user, device, or session. As Zuiderveen Borgesius points out, "Many companies are not interested in tying a name to data they process for behavioural targeting, even though they could easily do so."[37]

Supposedly anonymized datasets are rarely safe against re-identification. In many cases, even a handful of seemingly benign data points are enough to uniquely identify a person.[38] Similarly, fingerprinting can often uniquely identify a device using its settings.[39]

Given the above, it is crucial that data protection law protects data subjects against these dangers. Its very purpose is to safeguard individuals from the misuse of their personal data, which is a fundamental right. Tracking practices, as outlined, not only infringe upon this right but also pose a significant threat to the autonomy and dignity of individuals. The covert accumulation and exploitation of personal data through tracking mechanisms enable manipulation and discrimination, undermining the essence of individual freedom and self-determination.

4. Grounds for the complaint

Based on the facts presented above, I am of the opinion that the controller has violated data protection law, as I will explain in the following.

4.1. Violation of Art. 6(1) GDPR: Lawfulness of processing

The tracking data transmissions listed in Section 2.2 fall within the scope of the GDPR but the controller had no legal basis for this processing.

4.1.1. Transmission of tracking data falls under the GDPR

Through the tracking data transmissions, the controller processed my personal data by automated means. Accordingly, they fall within the scope of the GDPR (Art. 2(1) GDPR).

---

purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you; Gille/Meineck/Dachwitz, Wie eng uns Datenhändler auf die Pelle rücken, 2023, https://netzpolitik.org/2023/europa-vergleich-wie-eng-uns-datenhaendler-auf-die-pelle-ruecken/

[35] Christl, Corporate Surveillance in Everyday Life, 2017, https://crackedlabs.org/en/corporate-surveillance

[36] Urban/Tatang/Degeling/Holz/Pohlmann, The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR, 2018, https://arxiv.org/pdf/1811.08660.pdf; Englehardt/Narayanan, Online Tracking: A 1-million-site Measurement and Analysis, 2016, https://dl.acm.org/doi/pdf/10.1145/2976749.2978313; Cyphers/Gebhart, Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance, 2019, https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance.pdf

[37] Zuiderveen Borgesius, Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation, 2016, p. 268

[38] cf. e.g. Rocher/Hendrickx/de Montjoye, Estimating the success of re-identifications in incomplete datasets using generative models, Nature Communications, 2019, https://www.nature.com/articles/s41467-019-10933-3

[39] Ischatzkin/Budington/maximillianh/Antaki, About Cover Your Tracks, 2021, https://coveryourtracks.eff.org/about

The European Court of Justice has repeatedly and consistently stressed that the concept of personal data is to be interpreted broadly[40], including in the context of online advertising and tracking[41]. The definition of "personal data" in Article 4(1) of the GDPR explicitly lists online identifiers as a possible means of identification. Recital 26 of the GDPR further confirms: "To determine whether a natural person is identifiable, all means should be considered that could likely be used by the controller or any other person, according to general estimates, to directly or indirectly identify the natural person, such as singling out." It was specifically the legislature's intention to make it clear that the GDPR applies in the context of online tracking[42]:

> "Data subjects can be indirectly inferred for example through 'singling out' as mentioned in Recital 26 GDPR. The *European Parliament* had pushed for this clarification, since in the online world, for example with the help of cookies, IP addresses, browser fingerprints and other techniques, personality profiles are generated for many users by which they receive individual advertising without the operators of such advertising networks needing their civil names."

Therefore, the mere possibility of individualizing or recognizing an individual based on a piece of data suffices for the presence of personal data.[43]

The tracking services integrated by the controller have all read and/or set IDs that are used to identify me and my device. These IDs are specifically designed to be unique and avoid collisions, ensuring that they will only ever be assigned once and thus precisely identify me. For example, one common ID format that trackers often use are UUIDs/GUIDs. Those are explicitly specified to "guarantee uniqueness across space and time."[44] One would have to generate 1 billion UUIDv4s per second for about 86 years to have even just a 50 % probability of a collision.[45]

---

[40] cf. e.g. European Court of Justice, Judgment of 20 December 2017, Case C-434/16, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0434; European Court of Justice, Judgment of 4 May 2023, Case C-487/21, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0487; European Court of Justice, Judgment of 7 March 2024, Case C-479/22 P, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0479

[41] European Court of Justice, Judgment of 7 March 2024, Case C-604/22, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0604

[42] Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 1. edition, 2017, Part 3, mn. 3 (translated)

[43] in agreement: Farinho in Spiecker gen. Döhmann/Papakonstantinou/Hornung/De Hert, General Data Protection Regulation, Art. 4(1) Personal data, 2023, mn. 21, 24; Zuiderveen Borgesius, Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation, Computer Law & Security Review 2016, 256; Article 29 Data Protection Working Party, WP 136: Opinion 4/2007 on the concept of personal data, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, p. 14; Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 1. edition, 2017, Part 3, mn. 3; Karg in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. edition, 2019, Art. 4 Nr. 1 DSGVO, mn. 49–50; Schantz in Schantz/Wolff, Das neue Datenschutzrecht, 1. edition, 2017, chapter C.II, mn. 292–293; Schild in BeckOK Datenschutzrecht, 45. edition, 2023, Art. 4 Nr. 1, mn. 17, 19

[44] Leach/Mealling/Salz, RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace, 2005, https://datatracker.ietf.org/doc/html/rfc4122

[45] Wikipedia contributors, Universally unique identifier, 2024, https://en.wikipedia.org/w/index.php?title=Universally_unique_identifier&oldid=1212321712

Additionally, trackers commonly share IDs among each other (a process referred to as "cookie syncing" on the web).[46] This process allows different tracking services to share and match IDs with each other, thereby combining data from various sources to create an even more comprehensive profile of an individual.

These IDs are then used not only to collect data about individuals and track their behaviour, but for example also to deliver targeted advertisements.

As such, it is apparent that the IDs' very purpose is to single out users as referred to in Recital 26 GDPR and identify them.

Even if the IDs themselves were not personal data on their own, the transmitted tracking data as whole unequivocally constitutes personal data. A controller does not need to be able to immediately infer a data subject's name from some information for that information to be personal data.[47]

In the context of online tracking and advertising, IDs are never processed on their own. Instead, they are combined with other information, such as interaction data, browsing history, location data, device parameters, behavioral patterns, and IP addresses, to create detailed fingerprints and profiles of users and target them with personalized ads. As shown in Section 2.2, the very purpose of the trackers that the controller embedded into the app is to target and/or recognize individual users. In this larger context, there is an overwhelming consensus among legal scholars that such data processing falls under the scope of the GDPR and constitutes personal data.[48] This is in line with Recital 30 GDPR.

This position is further supported by a large corpus of guidelines and decisions by various data protection authorities. These are outlined in the Appendix in Section A2. and Section A3., respectively.

---

[46] Urban/Tatang/Degeling/Holz/Pohlmann, The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR, 2018, https://arxiv.org/pdf/1811.08660.pdf; Englehardt/Narayanan, Online Tracking: A 1-million-site Measurement and Analysis, 2016, https://dl.acm.org/doi/pdf/10.1145/2976749.2978313; Cyphers/Gebhart, Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance, 2019, https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance.pdf

[47] Farinho in Spiecker gen. Döhmann/Papakonstantinou/Hornung/De Hert, General Data Protection Regulation, Art. 4(1) Personal data, 2023, mn. 20; Purtova, From knowing by name to targeting: the meaning of identification under the GDPR, 2022, https://academic.oup.com/idpl/article/12/3/163/6612144; EU FRA, Handbook on European data protection law, 2018 edition, section 2.1, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf; Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 1. edition, 2017, Part 3, mn. 3; Arning/Rothkegel in Taeger/Gabel, DSGVO - BDSG - TTDSG, 4. edition, 2022, Art. 4 DSGVO, mn. 24, 30; Ernst in Paal/Pauly, DS-GVO BDSG, 3. edition, 2021, Art. 4 Nr. 1 DSGVO, mn. 8; Karg in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. edition, 2019, Art. 4 Nr. 1 DSGVO, mn. 48–49; Klabunde in Ehmann/Selmayr/Klabunde, DS-GVO, 2. edition, 2018, Art. 4 DSGVO Nr. 1, mn. 18; Schantz in Schantz/Wolff, Das neue Datenschutzrecht, 1. edition, 2017, chapter C.II, mn. 291–292; Schild in BeckOK Datenschutzrecht, 45. edition, 2023, Art. 4 Nr. 1, mn. 17; Ziebarth in Sydow/Marsch, DS-GVO/BDSG, 3. edition, 2022, Art. 4 Nr. 1 DSGVO, mn. 14; Karg/Kühn, Datenschutzrechtlicher Rahmen für "Device Fingerprinting" - Das klammheimliche Ende der Anonymität im Internet, ZD 2014, 285, p. 288; Wenhold, Nutzerprofilbildung durch Webtracking, 1. edition, 2018, chapter E.I.2, p. 130

[48] Gola in Gola/Heckmann, Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, 3. edition, 2022, Art. 4 Nr. 1 DSGVO, mn. 23; Klar/Kühling in Kühling/Buchner, DS-GVO/BDSG, 3. edition, 2020, Art. 4 Nr. 1 DSGVO, mn. 36; Schild in BeckOK Datenschutzrecht, 45. edition, 2023, Art. 4 Nr. 1, mn. 20

Finally, it bears mention that in all of the requests detailed in Section 2.2, the tracking company has the option to associate the transmitted tracking data with the user's IP address. As the European Court of Justice has repeatedly ruled, that information may make it possible to create a profile of that user and actually identify the person specifically concerned by such information.[49]

As a result, the information in the described tracking data transmissions is evidently personal data. Clearly, it was also processed by automated means and thus falls under the scope of the GDPR.

4.1.2. No legal basis is applicable for the transmissions

As per Art. 6(1) GDPR, the processing of personal data is only lawful if one of six possible legal bases is applicable. However, there is no possible valid legal basis for the processing carried out by the controller:

a. Consent (Art. 6(1)(a) GDPR): Consent can only be given by a statement or by a clear affirmative action (Art. 4(11) GDPR). Recital 32 GDPR clarifies that silence, pre-ticked boxes or inactivity do not constitute consent.

   As already explained, the transmissions detailed above happened without any interaction whatsoever. Thus, consent cannot possibly have been given for them. In any case, the burden of proving that consent has been given would be on the controller according to Art. 7(1) GDPR.
b. Necessity for performance of a contract (Art. 6(1)(b) GDPR): The described data transmissions were for the purposes of online tracking. Such processing is not necessary for the performance of a contract.

   In its *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, the EDPB explicitly confirms that Art. 6(1)(b) GDPR cannot be used as a legal basis for tracking and profiling users[50], online behavioural advertising[51], or collecting metrics for "service improvement"[52].
c. Legal obligation (Art. 6(1)(c) GDPR): obviously not applicable.
d. Necessity for protection of natural person's vital interests (Art. 6(1)(d) GDPR): obviously not applicable.
e. Necessity for performance of a task carried out in the public interest (Art. 6(1)(e) GDPR): obviously not applicable.
f. Necessity for purposes of legitimate interests (Art. 6(1)(f) GDPR): The controller also cannot claim a legitimate interesting in the processing. Legitimate interests are typically not a suitable legal basis for tracking.[53] It is not apparent why the controller's interest in tracking would outweigh my interests or fundamental rights and freedoms.

[49] cf. e.g. European Court of Justice, Judgment of 7 March 2024, Case C-604/22, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0604; European Court of Justice, Judgment of 17 June 2021, Case C-597/19, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62019CJ0597; European Court of Justice, Judgment of 19 October 2016, Case C-582/14, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0582

[50] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf, mn. 56

[51] ibid., mn. 51 et seq.

4.2. Violation of Art. 25 GDPR and Art. 5(1)(c) GDPR: Data protection by design and by default, data minimisation

The controller has failed to implement appropriate technical and organisational measures to ensure data protection by design and by default as required by Art. 25 GDPR.

Art. 25(1) GDPR requires the controller to implement appropriate measures at the time of determining the means of processing as well as during the processing itself. This includes measures to effectively implement the data minimisation principle as per Art. 5(1)(c) GDPR.[54] The EDPB has confirmed that this obligation applies to all controllers, regardless of their size or the complexity of their processing operations.[55]

Section 2.2 details the tracking that the app has performed. As explained in Section 3, the online tracking ecosystem presents severe risks to the rights and freedoms of data subjects, even if only seemingly beneign data is being processed. It is the controller's obligation to take the current 'state of the art' into account in their risk analysis and have knowledge of how technology can present data protection risks.[56] They should have been aware of these risks as they are widely documented and discussed in literature, media, and public debate.

However, they have failed to mitigate these risks, instead enabling unnecessary collection and transmission of data by default. The controller has included the above mentioned third-party tracking SDKs into their app and configured them to send tracking payloads without any user interaction.

The controller cannot argue that the SDKs themselves configured the tracking to be enabled by default, either. It is the controller's responsiblity to make sure that functions that do not have a legal basis or are not compatible with the intended purposes of processing are switched off when including third-party software in their app.[57]

As explained in Section 4.1.2, the data collected through the tracking goes beyond what is adequate and necessary for the app's functionality. If the controller should argue that they need certain statistics for example to monitor the performance of their app, less granular, aggregated, or anonymized data would have sufficed for this purpose instead of combining

[52] ibid., mn. 48 et seq.

[53] cf. e.g. Datenschutzkonferenz, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021), Version 1.1, 2022, https://www.datenschutzkonferenz-online.de/media/oh/20221130_OH_Telemedien_2021_Version_1_1.pdf, Section IV. 5; Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, FAQ: Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps, Version 2.0.1, 2022, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/03/FAQ-Tracking-online.pdf, Section A.3.1; Article 29 Data Protection Working Party, WP 217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, p. 32; Article 29 Data Protection Working Party, WP 203, Opinion 03/2013 on purpose limitation, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, p. 46

[54] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, mn. 61

[55] ibid., mn. 6

[56] ibid., mn. 19, 30

[57] ibid., mn. 44

the data with unique identifiers that allow the controller and third-parties to identify me.[58] They have thus collected more data than is necessary, violating the principle of data minimisation as prescribed by Art. 5(1)(c) GDPR.

Finally, users cannot reasonably expect that apps transmit such detailed identifiable data about them without any interaction.[59]

4.3. Burden of proof

As a data subject, I have no insights into the internal processes and data processing practices of either the controller or the tracking companies the controller has integrated into their app. Consequently, the burden of proof falls on the controller.

This is regulated in Art. 5(2) GDPR.[60] It was further explicitly confirmed by the European Court of Justice.[61]

4.4. § 25 TTDSG: Privacy protection for terminal equipment

In addition to the GDPR, the controller has also violated § 25 TTDSG as the transposition of Art. 5(3) ePrivacy Directive into German law.

As shown in Section 2.2, the app has sent various information relating to used device to tracking companies. In order to do so, the app inevitably had to read the information from the terminal equipment[62], thus opening the scope of § 25 TTDSG. Unlike the GDPR, the TTDSG doesn't just cover personal data but any data that is read from or stored on an end user's terminal equipment.[63] The TTDSG does not include any significance threshold on the types of data concerned, either—any information can fall within its scope, including purely technical information.[64]

The storing of information, or the gaining of access to information already stored in the terminal equipment of a user requires the user's consent on the basis of clear and comprehensive information according to § 25(1) TTDSG.

While the TTDSG does list two exceptions to that rule in § 25(2) TTDSG, neither of them is applicable in this case:

a. As set out above, the information was sent to tracking and/or advertising companies. As such, the purpose of accessing this information was expressly *not* the transmission of a

[58] ibid., mn. 49, 75

[59] ibid., mn. 70

[60] with additional references: Schantz in BeckOK Datenschutzrecht, 45. edition, 2023, Art. 5, mn. 39

[61] European Court of Justice, Judgment of 24 February 2022, Case C-175/20, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62020CJ0175

[62] Schürmann/Guttmann in Auernhammer, DSGVO/BDSG, 8. edition, 2023, § 25 TTDSG, mn. 27, 31, 37; EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, 2023, https://www.edpb.europa.eu/system/files/2023-11/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_en.pdf, mn. 29, 31, 35, 39

[63] EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, 2023, https://www.edpb.europa.eu/system/files/2023-11/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_en.pdf, mn. 7–12; Schneider in Assion, TTDSG, 2022, § 25 TTDSG, mn. 23

[64] Schürmann/Guttmann in Auernhammer, DSGVO/BDSG, 8. edition, 2023, § 25 TTDSG, mn. 20–23; Burkhardt/Reif/Schwartmann in Schwartmann/Jaspers/Eckhardt, TTDSG, 1. edition, 2022, § 25 TTDSG, mn. 29

message over a public telecommunications network. The exception in § 25(2)(1) TTDSG only applies where the transmission of a message over a public telecommunications network would not be possible at all without the storing of or the access to the concerned information[65], and is thus not applicable here.

b. Likewise, the controller cannot claim that the access was absolutely necessary to provide a telemedia service expressly requested by me. The exception has to be interpreted narrowly, with tracking and advertising not being strictly necessary.[66] Thus, § 25(2)(2) TTDSG is not applicable either.

However, the controller has not obtained consent as there was no interaction with the app at all. § 25(1) TTDSG defers to the GDPR for conditions on consent. As such, the same reasoning as in Section 4.1.2 applies here as well.

5. Requests and suggestions

In the previous sections, I have explained why I believe that the controller has violated my data protection rights. Therefore, I am now addressing this complaint to you.

I ask you to investigate my complaint and to examine the described issues by means of your investigative powers according to Art. 58(1) GDPR.

I also ask you to inform me about the progress and outcome of the complaint procedure according to Art. 77(2) GDPR and Art. 57(1)(f) GDPR during the course of the complaint procedure, but at the latest within three months (cf. Art. 78(2) GDPR).

I finally ask you to make use of any supervisory measures that you deem necessary to mitigate the controller's violation of my rights in line with your corrective powers as per Art. 58(2) GDPR. In doing so, please consider that the described violations in all likelihood do not just apply to me, but to all users of the app.

6. Concluding remarks

You may share my data with the controller for the purpose of processing the complaint.

---

[65] Schürmann/Guttmann in Auernhammer, DSGVO/BDSG, 8. edition, 2023, § 25 TTDSG, mn. 123; Schmitz in Geppert/Schütz, Beck'scher TKG-Kommentar, 5. edition, 2023, § 25 TTDSG, mn. 66; Hanloser in Gierschmann/Baumgartner, TTDSG, 1. edition, 2023, § 25 TTDSG, mn. 94; Nolte in Säcker/Körber, TKG – TTDSG, 4. edition, 2023, § 25 TTDSG, mn. 33

[66] Article 29 Data Protection Working Party, WP 194, Opinion 04/2012 on Cookie Consent Exemption, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf; Datenschutzkonferenz, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021), Version 1.1, 2022, https://www.datenschutzkonferenz-online.de/media/oh/20221130_OH_Telemedien_2021_Version_1_1.pdf, Section III. 3. c); Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, FAQ: Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps, Version 2.0.1, 2022, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/03/FAQ-Tracking-online.pdf, Section A.1.4; Schneider in Assion, TTDSG, 2022, § 25 TTDSG, mn. 36, 44; Nolte in Säcker/Körber, TKG – TTDSG, 4. edition, 2023, § 25 TTDSG, mn. 37; Burkhardt/Reif/Schwartmann in Schwartmann/Jaspers/Eckhardt, TTDSG, 1. edition, 2022, § 25 TTDSG, mn. 127, 140; Ettig in Taeger/Gabel, DSGVO - BDSG - TTDSG, 4. edition, 2022, § 25 TTDSG, mn. 56

If you need any more details, please feel free to contact me. You can reach me as follows:
kim.muster@example.tld
I agree to being contacted via unencrypted email.

Thank you in advance for your assistance.

Appendix

A1. Results from "TrackerControl" on my device

TODO

A2. DPA guidelines regarding personal data in the context of online tracking

Several DPAs have issued guidelines or guidance notes on the use of cookies and other tracking technologies which involve the processing of IDs that are uniquely assigned to a person. These guidelines universally confirm that such IDs are personal data under the GDPR, especially when they are used or combined to create profiles of individuals or to single them out from others.

For example, the DPC Ireland explains that cookies can include personal data such as usernames or unique identifiers like user IDs and other tracking IDs. The DPC adds that where cookies contain identifiers that may be used to target a specific individual, or where information is derived from cookies and other tracking technologies that may be used to target or profile individuals, this will constitute personal data and its processing is also subject to the rules set out in the GDPR. The DPC also emphasizes that online identifiers are included in the definition of personal data in Article 4(1) of the GDPR, and that it does not matter whether the controller is in possession of other information that may be needed to identify an individual; the fact that the person may be identified, even with the addition of information held by another organisation, is sufficient to make this data personal data.[67]

In an FAQ on Google Analytics, the Danish Datatilsynet also adopts a broad understanding of personal data in relation to online identifiers. It states that a unique identifier makes it possible to identify the individual to whom the data relates, even if it is not possible to assign a specific name or identity to the person concerned. It cites the GDPR's explicit mention of the "singling out" concept.[68]

In its opinion on the interplay between the ePrivacy Directive and the GDPR, the EDPB mentions cookies as a clear example of processing activities which trigger the material scope of both the ePrivacy Directive and the GDPR.[69]

Similarly, in its guidelines on telemedia, the German Datenschutzkonferenz states that the use of cookies and other tracking technologies often involves the processing of personal

[67] DPC Ireland, Guidance Note: Cookies and other tracking technologies, 2020, https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf

[68] Datatilsynet, Google Analytics, https://www.datatilsynet.dk/english/google-analytics

[69] EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, 2019, https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

data and thus fall within the scope of both the TTDSG (the German law implementing the ePrivacy Directive) and the GDPR.[70]

A3. DPA decisions regarding personal data in the context of online tracking

Some DPAs have also issued decisions on specific cases involving the processing of IDs that are uniquely assigned to a person, again confirming that the processing of unique IDs in the context of online tracking falls under the scope of the GDPR.

For example, the Swedish DPA (IMY) issued a decision in June 2023, fining Tele2 Sverige AB and three other website providers for using Google Analytics despite the EU recommendations and decisions and without implementing additional safeguards.[71] In the decision, the IMY explains that network/online identifiers can be used to identify a user, especially when combined with other similar types of information.[72] The IMY considered the data collected by Google Analytics, such as unique identifiers stored in the cookies `_gads`, `_ga`, and `_gid`, IP addresses, and other information related to the website visit and user's browser. They highlight that these identifiers were created with the express aim of being able to distinguish individual visitors, thus making them identifiable. The IMY notes that even if the IDs alone did not make individual identifiable, the IDs in combination with the other transmitted data makes website visitors even more distinguishable. As such, they conclude that the transmitted data information constitutes personal data. The IMY explains that this differentiation is in itself sufficient to make the visitor indirectly identifiable in accordance with Recital 26 GDPR and that knowledge of the visitor's name or physical address is not required. They also do not consider it necessary that the controller or processor actually intends to identify the visitor, noting that the possibility of doing so is in itself sufficient to determine whether it is possible to identify a visitor.[73]

Similarly, the Austrian DPA (DSB) issued a decision in December 2021, finding that an Austrian website violated the GDPR by transferring personal data to the US by using Google Analytics. The DSB notes that the cookies used by Google Analytics, `_ga`, `_gid`, and `cid`, contained unique identifiers that were stored on the users' devices and browsers, and that only through these identifiers was it possible for the website operator and Google to distinguish visitors as well as determine whether they had visited the website before. The DSB explains its position that such a possibility of individualizing website visitors was sufficient to open the scope of data protection law and that being able to find out the person's name was

[70] Datenschutzkonferenz, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021), Version 1.1, 2022, https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf

[71] At the same time, the IMY also issued three additional, very similar decisions, against other websites: DI-2020-11397 (https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-ga-cdon.pdf), DI-2020-11368 (https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-ga-coop.pdf), DI-2020-11370 (https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-ga-dagens-industri.pdf)

[72] IMY, Beslut efter tillsyn enligt dataskyddsförordningen – Tele2 Sverige AB:s överföring av personuppgifter till tredjeland, DI-2020-11373, 2023, https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-ga-tele2.pdf, p. 10

[73] ibid., p. 11

not necessary, citing Recital 26 GDPR as justification.[74] With regards to the controller's and Google's argument that they didn't actually intend to associate the IDs with an actual person, the DSB underlines[75]:

> "Insofar as the defendants argue that no 'means' are used to link the identification numbers in question here to the person of the complainant, it must be reiterated that the implementation of Google Analytics on [the website] *results in* a singling out within the meaning of Recital 26 GDPR. In other words: Those who use a tool that only enables such singling out *in the first place*, cannot take the position that they do not 'reasonably' use any means to make natural persons identifiable."

The DSB also notes that these identifiers could combined with other information, such as browser data and IP addresses, which made the website visitors even more identifiable, referring to Recital 30 GDPR. The DSB further points out that Google Analytics was specifically designed to be implemented on as many websites as possible, in order to collect information about website visitors. They conclude that the data processed by Google Analytics constituted personal data and stress that not applying the GDPR to the processing done by Google Analytics would run afoul of the fundamental right to data protection.[76]

The DSB's decision was later confirmed by the Austrian Federal Administrative Court in judgement W245 2252208-1/36E, W245 2252221-1/30E[77].

In a more recent decision in March 2023, the DSB found that the use of Facebook's tracking pixel by an Austrian website provider also violated the GDPR and the ECJ's *Schrems II* judgement. In the decision, the DSB follows the same argument as in the Google Analytics decision, quoting from it with regards to the classification of tracking data as personal data.[78]

Again concerning Google Analytics but also Google Tag Manager, Tietosuojavaltuutetun toimisto, the Finish DPA, issued a decision in December 2022 against the public library online services of four cities in Finland. The decision mentions that personal data was collected through those tools.[79]

The CNIL, the French DPA, issued a decision in March 2022, ordering three French websites to comply with the GDPR in relation to their use of Google Analytics. The CNIL explains that online identifiers, such as IP addresses or information stored in cookies, could be used as a means of identifying a user, especially when combined with other similar types of in-

---

[74] Österreichische Datenschutzbehörde, Teilbescheid D155.027 2021-0.586.257, 2021, https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf, p. 27–28

[75] ibid., p. 28 (translated)

[76] ibid., p. 29

[77] https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20230512_W245_2252208_1_00/BVWGT_20230512_W245_2252208_1_00.pdf

[78] Österreichische Datenschutzbehörde, Bescheid D155.028 2022-0.726.643, 2023, https://noyb.eu/sites/default/files/2023-03/Bescheid%20redacted.pdf

[79] Tietosuojavaltuutetun toimisto, Apulaistietosuojavaltuutetun päätös käsittelyn lainmukaisuutta, käsittelyn turvallisuutta, sisäänrakennettua ja oletusarvoista tietosuojaa, rekisteröityjen informointia ja henkilötietojen siirtoa kolmansiin maihin koskevassa asiassa, 4672/161/22, 2022, https://finlex.fi/fi/viranomaiset/tsv/2022/20221663

formation, citing Recital 30 GDPR. The CNIL explains that the websites had to demonstrate the means implemented to ensure that the identifiers collected were anonymous, otherwise they could not be qualified as anonymous. They also note that the IDs used by Google Analytics were unique identifiers that were intended to differentiate between individuals and that these identifiers could also be combined with other information, such as the address of the site visited, metadata relating to the browser and operating system, the time and data relating to the visit to the website, and the IP address. The CNIL argues that this combination reinforced their distinguishing nature and made the visitors identifiable. The CNIL believes that the scope of the right to data protection would be diminished if this were decided otherwise.[80]

The CNIL also sanctioned Criteo, an online advertising company, with a fine in June 2023 for failing to verify that users from whom it processed data had given their consent. The CNIL considers that Criteo processed personal data, given the number and diversity of the data collected and the fact that they were all linked to an identifier, which made it possible, with reasonable means, to re-identify the natural persons to whom this data relates. The CNIL also notes that the Criteo cookie ID was intended to distinguish each individual whose data it collected and that a large amount of information intended to enrich the user's advertising profile was associated with this identifier. The CNIL believes that even if Criteo did not directly have the identity of the person associated with a cookie ID, reidentification could be possible if Criteo also collected other data such as the email address, the IP address, or even the user agent (or hashed forms thereof). The CNIL concludes that as long as Criteo is able to re-identify individuals using reasonable means, the processed data is personal data under the GDPR.[81]

The Norwegian Datatilsynet published a draft decision in May 2021, notifying Disqus, a company that provides a platform for online comments, that it would be fined for unlawfully processing personal data for programmatic advertising. The DPA states that online identifiers, such as cookie IDs, were personal data, as they enabled the controller to distinguish one website user from another, and to monitor how each user interacts with the website, citing Art. 4(1) GDPR and Recital 30 GDPR to support its interpretation.[82]

Finally, the DPA of Lower Saxony in Germany (LfD NDS) issued a decision in May 2023 concerning the use of a "pay or okay" system by Heise, a German tech news site. The site made users choose between paying for a monthly subscription or agreeing to their data being processed for advertising and other purposes. The LfD found that the requirements for obtaining consent were not fulfilled by Heise. In the decision, the LfD describes the high number of observed local storage objects, tracking techniques and third-party services used on the site, explaining that they will not provide a legal assessment of each one as a result.

[80] CNIL, Décision n° […] du […] mettant en demeure […], 2022, https://www.cnil.fr/sites/cnil/files/atoms/files/med_google_analytics_anonymisee.pdf, p. 4

[81] CNIL, Délibération SAN-2023-009 du 15 juin 2023, 2023, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000047707063

[82] Datatilsynet, Advance notification of an administrative fine – Disqus Inc., 20/01801-5, 2021, https://www.datatilsynet.no/contentassets/8311c84c085b424d8d5c55dd4c9e2a4a/advance-notification-of-an-administrative-fine--disqus-inc.pdf, p. 15–16

The LfD notes that Heise processed personal data through these objects, citing for example that Adform placed a `cid` cookie, which they determined to be an ID based on the name.[83]

[83] Die Landesbeauftrage für den Datenschutz Niedersachsen, Beschwerdeverfahren gegen Verarbeitungen personenbezogener Daten bei der Nutzung der Webseite www.heise.de, 2023, https://noyb.eu/sites/default/files/2023-07/11VerwarnungPurAboModellfinalgeschwrztp_Redacted.pdf, p. 6