# FAST TRACK TO SURVEILLANCE

## FREQUENTLY ASKED QUESTIONS

## Contents



## What is your coordinated action against Google about?

Through a combination of deceptive design, unclear language, misleading choices and missing information, Google's account signup process is designed to get consumers to allow an extensive and invasive processing of their personal data.

Google is not providing privacy by design and by default and processing personal data in a fair, lawful and transparent manner, as required by EU data protection law. Instead, Google is steering people towards its surveillance system where everything they do is monitored and exploited by the digital behemoth.

The Google account is the red thread which connects how users' data is used across all Google services. It is during this sign-up process that consumers take critical decisions about the settings of their account, with significant consequences as to how Google will process their personal data, including to profile them and target them with advertising. It is the company's extensive and invasive tracking, profiling and ad-targeting practices that fuel its advertising revenue, and that have made of Google one of the undisputed heavyweights of 'surveillance capitalism', with 81% of its revenue coming from ads.[1]

## What specific problems are there in the Google account signup process?

At the very beginning of the signup process, consumers must choose between 'Express personalisation' (one step) and 'Manual personalisation' (five steps). The personalisation refers to the consumer's preferences for the following three settings:

- *Web & App Activity*, which collects data from user activity across all Google services, including data from Chrome, search history, location data from Google Maps, and any website or app the consumer has interacted with which uses Google services,
- *YouTube history*, which keeps track of the videos searched and watched on YouTube,
- *Ad personalization*, which enables the use of all data collected to deliver targeted, personalised adverts.

[1] Statista.com, 'Biggest revenue source of leading online and tech companies in most recently reported quarter ending March 2022' (May 2022, accessed 10 June 2022).

The 'Express' option turns 'on' all settings in one step. If a consumer wants to switch anything 'off' to have better privacy protection, this takes them five steps with 10 clicks, grappling with unclear, misleading and incomplete information. In other words, rather than privacy by design, what Google provides is a fast track to surveillance. Also, turning 'off' all the settings is a much longer process than turning them 'on'. This is a 'dark pattern' that steers consumers into consenting to very extensive and invasive data collection and favouring Google's own interests.

Beyond the first step in the registration process, regardless of the option chosen – 'Express' or 'Manual' – consumers are faced with unclear, incomplete, and misleading information related to what Google does with their data. Important information particularly about data processing purposes and about the options that the user can choose from is either not presented up front, vague or missing. Google also frames the more privacy-friendly options as ones where consumers will miss out on advantages.

Consumers' data is not collected for specified, explicit and legitimate purposes, as required by the law. Instead, Google relies on oversimplified and vague purposes, and does not limit the collection and storage of data to the minimum necessary. Consumers cannot take an informed decision when they make their choices. Consent given is therefore not valid and Google lacks another valid legal basis for processing the personal data.

All these issues result in unfair, non-transparent and unlawful processing of consumers' personal data and run contrary to EU data protection rules.

## Does Google fully protect your privacy and personal data if you turn 'off' all settings?

Google's entire business model is based on exploiting personal data for various purposes, such as ad targeting and personalisation of content. This is how it has become one of the world's largest, most profitable companies in the world.

The Google account serves to unify and personalise the user's experience across all of Google's services. To use the company's services, the consumer has to accept its privacy policy and have their personal data processed in different ways for a myriad of purposes.

Our action is focused on the Google account registration process, but there are issues identified which relate to broader problems with Google's privacy policy, such as the vagueness of the processing purposes described in the policy. These issues cannot simply be addressed through a user turning 'off' a certain setting in their account. Moreover, Google's surveillance practices also affect non-registered Google users i.e. people who use or interact with Google services without a Google account.

For example, through its real time bidding ad system, Google provides over a thousand firms in Europe (1,058) with data such as what people are viewing or doing on a website, or app, 42 billion times every day.[2] Google sends 19.6 million broadcasts about German internet users' online behaviour every minute that they are online.[3]

## What do you want to achieve with this action?

We want Google to fully respect EU data protection rules and ensure that choosing privacy is the default and easiest choice when setting up a Google account. Nearly everybody is in one way or another exposed to Google's unfair practices. Data protection and privacy are fundamental rights in the EU. Forcing Google to fully respect these rights and act lawfully would be a major and long overdue step in fighting the surveillance economy.

At least tens of millions, if not hundreds of millions, of Europeans use Google services and many of these consumers probably also have a Google account.

While Google boasts that that "users are in control" of the data that the company collects and how it is used, a closer look reveals that it is actually the opposite – it is the tech giant that is in control the whole way.

Regardless of the path the consumer chooses when setting up an account, Google's data processing is opaque and unfair. Beyond steering users towards enabling privacy invasive settings, information crucial for users to make an

[2] Irish Council for Civil Liberties, 'The Biggest Data Breach: ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe' (16 May 2022, accessed 17 June 2022).
[3] Ibid.

informed choice regarding their options is either not presented up front, vague or missing. Moreover, consumers' data is not collected for specified, explicit and legitimate purposes. Contrary to what the GDPR requires, Google relies on oversimplified and vague purposes, and it does not limit the collection and storage of data to the minimum necessary. In this context, it is impossible for the consumer to make informed decisions and be in control of what happens with their data.

## How were the organisations taking part in this action chosen?

All BEUC members can participate in its coordinated actions. It is up to the individual consumer organisations to decide whether to participate. Members take this decision on a case-by-case basis according to their resources, capacity, expertise and priorities.

## Is the problem you are denouncing not fixed with Google's 'decline all' cookies option?

No. Our action does not relate to cookie banners that pop up when accessing Google services on the internet. It relates to the process for signing up to a Google account. These are two different things.

A cookie banner only affects the cookies that are placed on a user's device, for example your computer or smartphone, when accessing a specific website. Though cookies are used by Google to track consumers across the web and across different devices, the Google account is far more centralised, comprehensive and far reaching from a data processing perspective and has a different function than individual website cookie banners. In fact, if you are signed-in to your Google account, you won't be presented with a cookie banner when accessing Google services on the web such as YouTube.

Through a Google account, the company can track the consumer and connect how their data is used across all Google services. Some Google services – such as Gmail and the Play Store in fact require a Google account before they can be accessed.

It is during the account signup process that consumers take critical decisions about the settings of their Google account, with significant consequences as to how Google will process their personal data, including to profile them and target them with advertising.

## What other problems do you see with Google in the EU?

Besides the fact that Google is a repeat offender when it comes to the respect of EU data protection and privacy laws,[4] it has also already been found to be in breach of EU antitrust rules.[5] Moreover, additional complaints and investigations regarding the company are still pending both in relation to data protection and to competition concerns.

Google has a giant presence in many key digital markets, including mobile operating systems, online search, maps, email, internet browsers, video-sharing, etc. and is undisputedly one of the companies at the forefront of the 'surveillance economy'. Its data exploitation practices and business model set surveillance as the bedrock of digital markets.

## What happens now that you have filed these complaints?

We expect that the competent data protection authorities will fully investigate Google's practices, and use all their powers under the GDPR to determine whether Google's processing of account holders' personal data is lawful.

Given that Google's practices affect consumers across the EU and consumer organisations and data protection authorities in various EU member states are involved, along with the fact that Google has its main establishment in Ireland, we now expect to see a procedure launched under the GDPR's Cooperation mechanism (Article 60 GDPR). We

[4] On January 21, 2019, the French National Commission on Informatics and Liberty (CNIL), fined Google €50 million for lack of transparency, inadequate information, lack of valid consent regarding ads personalisation. It also issued a €90 million fine against the company on 31 December 2021 over the inability to allow YouTube users in France to refuse cookies as easily as they could accept them. On 26 June 2019, BEUC member UFC-Que Choisir filed a collective redress case in France against Google for consent violations under GDPR. This case is still pending. In another case, four US attorney-generals are suing Google for allegedly misleading users about when the company was able to track their location.
[5] For example, see the Google Shopping and Google Android cases.

hope that this mechanism will work better than for previous complaints we launched in 2018 (please see below in the next question). We consider this case of strategic importance for which cooperation between data protection authorities should be prioritised and supported by the European Data Protection Board, in line with the recent commitments announced in the "Vienna declaration."

## How does this action tie with a previous complaint launched by the BEUC network against Google?

In November 2018, BEUC and seven of its members launched a coordinated GDPR enforcement action regarding Google's location tracking practices, filing complaints with data protection authorities in multiple countries. Over three and a half years later, those complaints are currently in the hands of the Irish Data Protection Commission and remain unresolved. There has been no action yet by the authorities to improve the situation on the ground for consumers.

There are similarities in some of the issues raised in the complaints from 2018 and this new action. However this time, we have examined Google's practices from a broader perspective. While the 2018 complaints focused exclusively on the processing of location data when registering a Google account on an Android phone, this new action addresses the overall account signup process. The scope of the new action is therefore broader. There is no specific focus on a particular category of personal data, as was the case with the previous action which focused on location data.

Also, Google has introduced changes to the account registration process since November 2018 which deserve greater scrutiny. This new action therefore aims to test the functioning of the GDPR cooperation mechanism again and see if it works better than it has in our previous complaints.

## Is it time to reform the GDPR's enforcement system?

At the moment, enforcement of the GDPR for cross-border cases against Big Tech companies has been disappointing. Our complaints against Google's location-tracking from 2018 have not yet led to any action from the authorities that has improved the situation for consumers. More complaints are currently stuck, principally with the Irish Data Protection Commission, which is the country in the EU where many Big Tech companies are based.

However, we still believe that the GDPR's enforcement can and must be improved within the framework of the existing system and there is no need for a complete reform of the GDPR. BEUC[6] and civil society organisations more broadly,[7] have already put forward recommendations for improvements. Data protection authorities have also undertaken different initiatives to improve the situation.[8]

## What is your advice to consumers today?

The best that consumers can do is to rely on products and services which are more privacy-friendly than Google's, and use privacy-enhancing tools, such as browser add-ons to prevent online tracking. If consumers have no choice or decide to use Google's services and set up a Google account, they must be very careful with the settings they choose in their account.

Consumers should however be aware that these measures will not be enough to solve all existing issues. Enforcement authorities must step in to ensure Google fully complies with EU data protection law.

Google is one of the heavyweights of surveillance capitalism. Its business model relies on hoovering up and exploiting consumers' personal data. It is doing so in suspected breach of privacy and data protection laws and is a repeat offender. Instead of providing privacy by design and by default, as required by law, it is steering consumers towards surveillance by design and forcing them to navigate through a mix of unclear and misleading options if they want more privacy-friendly settings.

---

[6] BEUC, 'The long and winding road: Two years of the GDPR: A cross-border data protection enforcement case from a consumer perspective' (August 2020).
[7] Edri, 'Civil society call and recommendations for concrete solutions to GDPR enforcement shortcomings' (March 2022).
[8] EDPB, 'Statement on enforcement cooperation' (28 April 2022). See also EDPS conference 2022, 'The future of data protection - Effective enforcement in the digital world'.

In a fair market, all companies must abide by the rules and consumers should be empowered to choose between offers from legally compliant companies. But today, there is little choice effectively. Google's services play a central role in the lives of millions of consumers, and countless companies also rely on Google to do business. Even if a consumer chooses not to create a Google account, they may be obliged to create one when, for example, they buy a smartphone that uses Google's Android system, which almost 7 in 10 phones worldwide (69%) depend on,[9] if they want to download apps from the Google Play store. They may also be tracked and profiled by Google, even without a Google account.

[9] Statista.com, 'Mobile operating systems' market share worldwide from January 2012 to January 2022' (accessed 9 June 2022).