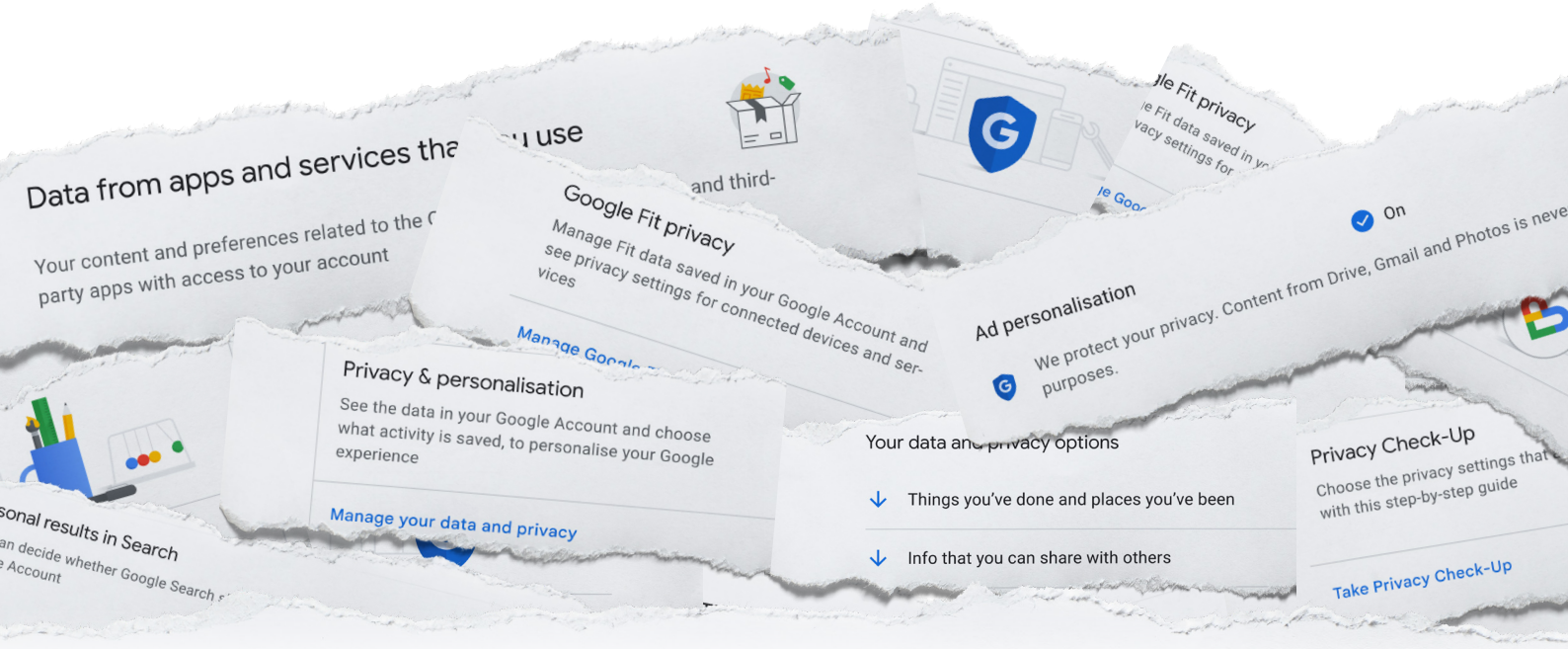
60 YEARS YOUNG YEARS STRONG

BEUC The European Consumer Organisation



Fast track to surveillance

How Google makes privacy the hard choice

Acknowledgements

We would like to thank AWO, an agency working to shape, apply and enforce data rights, for their legal support in the preparation of this action.

BEUC also wishes to thank its members and the data subjects involved in this action to better protect consumers' privacy and data.

BEUC also thanks the Publishing Bureau for designing this document and the visuals associated with this action.

Disclaimer

The contents of this document are based on a legal analysis of Google's practices carried out by BEUC and AWO between March and May 2022.

60 YEARS YOUNG YEARS STRONG

BEUC The European Consumer Organisation

June 2022

Rue d'Arlon, 80 Bte 1
B - 1040 Brussels
Tel: +32 2 743 15 90

Executive Summary

Our report shows that Google is unfairly steering consumers during its account signup process, so that they accept surveillance across all Google products and services. The signup process, which does not provide a simple, straightforward option for consumers to choose privacy-friendly settings, is plagued with deceptive design and unclear and misleading choices.

As a result a number of consumer organisations, under BEUC's coordination, are taking action including by filing GDPR complaints and asking data protection authorities to ensure that Google complies with EU data protection law.

Instead of 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, Google is steering people towards its surveillance system where everything they do is monitored and exploited by the digital behemoth.

Google provides a myriad of products and services, including the Android mobile operating system, Chrome browser, YouTube, Google Search, Gmail, Google Maps and the Google Play Store. Through a Google account, the company can unify and personalise the consumer's experience across all its services. Some Google services – such as Gmail and the Play Store – require a Google account before they can be accessed.

Google is unfairly steering consumers during its account signup process, so that they accept surveillance across all Google products and services.

It is during this 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.

During the account signup process, consumers must indicate their preferences on the following three settings:

Web & App Activity, which collects data from user activity across all Google services, including data from Chrome, search history, and Google Maps, and any website or app which uses Google services,

YouTube history, which keeps track of your searches and videos watched on YouTube,

Ad personalization, which enables the use of all data collected to deliver targeted, personalised adverts.

A legal analysis carried out by BEUC and AWO serves to substantiate BEUC's and its members' complaints that, much against Google's claim that users are in control of the data that the company collects and how it is used, the signup process is engineered to serve the company's interests and runs against EU data protection law in different ways:

- ***No data protection by design and by default:*** Google does not provide an 'express' option to let consumers switch these settings 'off' and choose the best possible protection for their privacy in one step. This takes them five steps with ten clicks, grappling with unclear, misleading and incomplete information. On the contrary, Google provides up front an 'express' option to switch everything 'on' in one step, encouraging users to quickly give Google permission to monitor and exploit everything the consumer does by making it the easiest choice.
- ***Un-transparent and unfair data processing, deceptive design and invalid consent:*** beyond the deceptive language Google uses at every step of the registration process, 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 cannot take informed decisions when they make their choices. The consent given is therefore not valid and Google lacks a valid legal basis for processing personal data.
- ***Breaches of purpose limitation, data minimisation and storage limitation principles:*** Consumers' data is not collected for specified, explicit and legitimate purposes. Google relies on oversimplified and vague purposes, and it does not limit the collection and storage of data to the minimum necessary.

All this results in unfair, non-transparent and unlawful processing of consumers' personal data.

> **Google and its parent company, Alphabet, have an enormous presence in many key digital markets and are at the forefront of 'surveillance capitalism'.**

Unfortunately, some of these issues are not entirely new. Many similar problems were already brought forward in the GDPR complaints filed by consumer organisations in November 2018 in relation to Google's processing of location data.[1] Over three and a half years later, those complaints are still pending with the Irish Data Protection Commission and Google's practices continue to run afoul of EU data protection law.

The Google account signup process not only has important repercussions for consumers' data protection and privacy rights, it also helps sets Google's surveillance as the bedrock for the digital market. There are tens of millions of Google accounts in existence in the EU and many companies rely on Google's products and services to do business.

Google and its parent company, Alphabet, have an enormous presence in many key digital markets (mobile operating systems, internet browsers, email, maps, search, video-sharing, etc.) and are at the forefront of 'surveillance capitalism'. Data protection authorities must step in and ensure that Google respects EU law.

1 BEUC press release, 'GDPR complaints against Google's deceptive practices to track user location' (27 November 2018) and Forbrukerrådet (Norwegian Consumer Council) report, 'Every step you take' (27 November 2018).

1 **Google's account signup process**: a core element of its commercial surveillance system

In November 2018, BEUC and its members launched a coordinated GDPR enforcement action against Google's location tracking practices.[2] Fast forward to June 2022 and those complaints still remain unresolved. A broader look into Google's account signup process, reveals that the company's practices continue to run afoul of EU data protection law.

Google is one of the most powerful and popular companies in the world. Its products and services, such as Android phones, the Chrome browser, YouTube, Google Search, Gmail, Google Maps, Google Play Store, are used daily by millions of consumers in the EU. Through a Google account, the company can track, unify and personalise the consumer's experience across all its services. Some Google services – such as Gmail and the Play Store – in fact require a Google account before they can be accessed.

> **The Google account signup process helps set the company's surveillance as the bedrock for the digital market, as many companies depend on Google for their day-to-day operations and services.**

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 allow its clients to target them with advertising.

2 BEUC press release, 'GDPR complaints against Google's deceptive practices to track user location' (27 November 2018).

In addition to tracking and monetising everything Google users do on its own services, like YouTube, Google Maps and Google Search, Google's analytics and ads tools and services are widely used by third parties across the web. A 2020 report found Google trackers in 87.5% of the EU sites that were analysed.

Through its real time bidding system and thanks to the data it collects, 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. Google sends 19.6 million broadcasts about German internet users' online behaviour every minute that they are online.[3]

Reports from Forbrukerrådet, a Norwegian consumer association and BEUC member, have shown how ubiquitous surveillance ads and commercial surveillance now are across the internet.[4]

In 2021, Google's revenue amounted to $256.7 billion (€225.6bn).[5] Over 80% of Google's revenue comes from advertising.[6] It is the company's extensive and invasive tracking, profiling and ad-targeting practices that fuel its advertising revenue, and that have made Google one of the undisputed heavyweights of 'surveillance capitalism'.

As one of the main entrances to the Google data mining universe and the red thread that connects everything Google users do, the Google account signup process not only has important repercussions for consumers' data protection and privacy rights, it also helps set Google's surveillance as the bedrock for the digital market, as many companies depend on Google for their day-to-day operations and services.

While Google boasts that 'users are in control' of the data that the company collects and how it is used, or that it 'never sells your personal information',[7] a closer look reveals that everything is engineered to steer users towards choosing surveillance by design and by default.

Choosing privacy is neither the fastest nor the easiest choice when setting up a Google account. It is in fact the contrary – Google provides a fast track to surveillance.

---

3 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).

4 Forbrukerrådet, '**Report: Out of Control**' (14 January 2020) and '**Time to Ban Surveillance-Based Advertising – The Case Against Commercial Surveillance Online**' (June 2021).

5 Statista.com, '**Annual revenue of Google from 2002 to 2021**' (February 2022, accessed 15 June 2022).

6 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).

7 Google Safety Center, '**Ads that respect your privacy**' (accessed 16 June 2022).

2 **Creating a Google Account**: Surveillance by design and by default

During the Google Account signup process, consumers must indicate their preferences on the following three settings:

Web & App Activity, which collects data from user activity across all Google services, including data from Chrome, search history, and Google Maps, from any website and app that uses Google services,

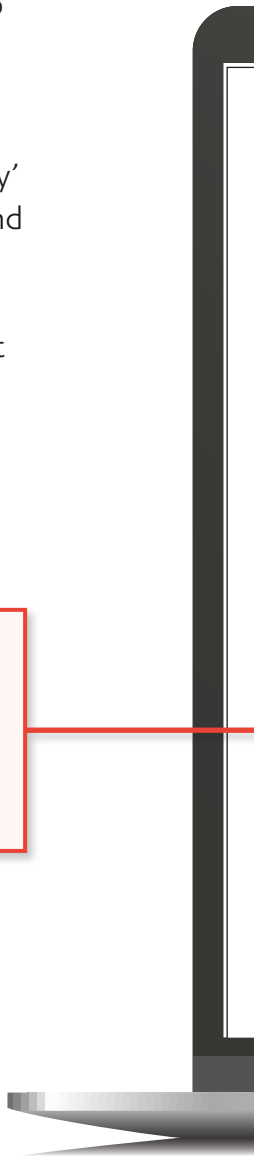
YouTube history, which keeps track of your searches and the videos watched on YouTube,

Ad personalization, which enables the use of all data collected to deliver targeted, personalised adverts.

The problems start at the very beginning of the process. Consumers are faced with two options: 'Express personalisation', which takes one step, or 'Manual personalisation', which takes five steps.

The 'Express personalisation' option turns on 'Web & App Activity', 'YouTube History' and 'Ad personalisation' in one simple step, giving Google permission to monitor and exploit everything the consumer does across its services. Google does not provide an 'express' option to switch everything off in one step. A consumer who wants to say no to certain data processing operations and better protect its privacy must opt for the 'Manual personalisation'. This takes five steps with 10 clicks, grappling with unclear, misleading and incomplete information, in a clear illustration of the 'dark pattern' which the European Data Protection Board refers to as 'longer than necessary'.[8]

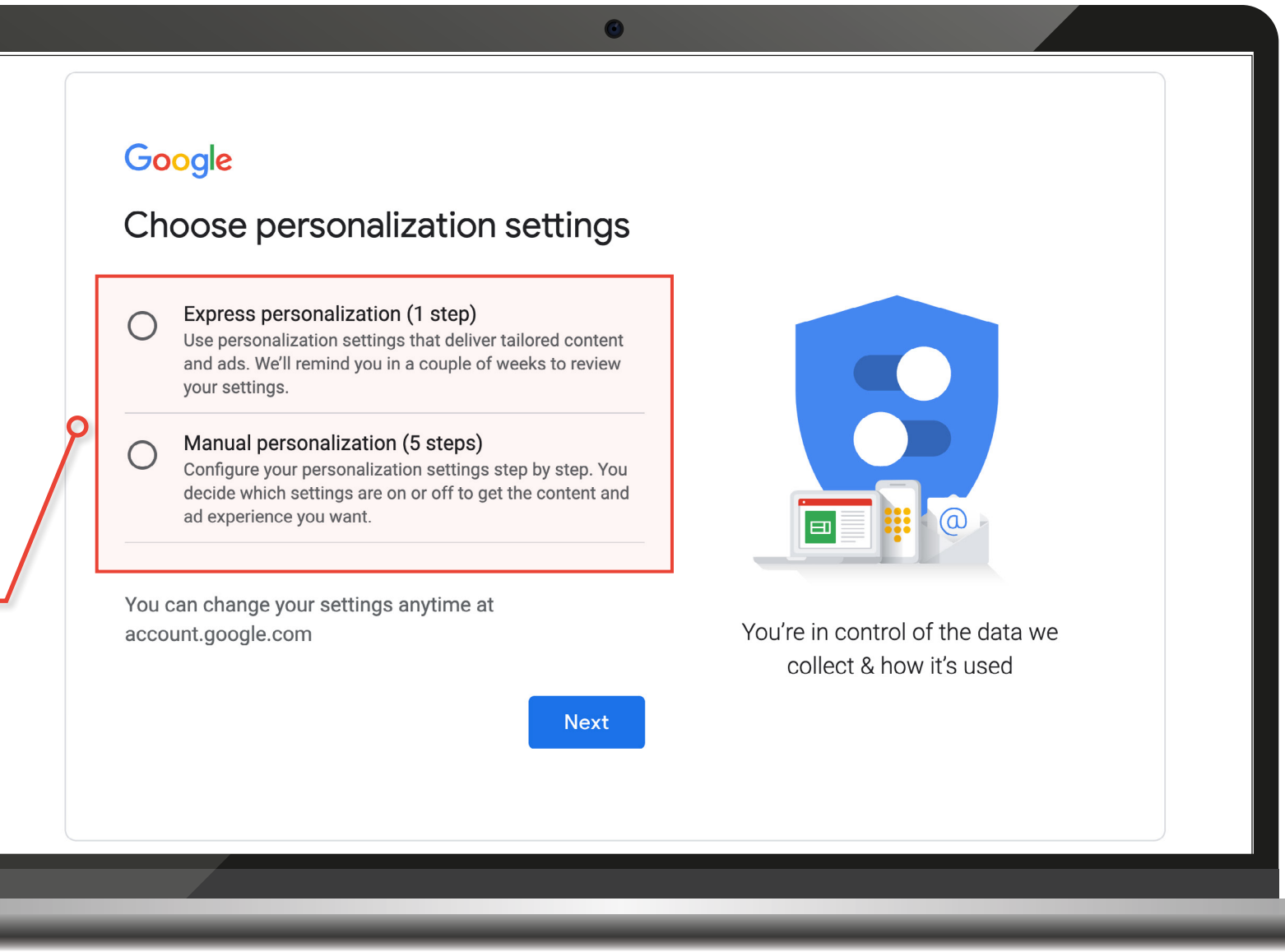
It is much more cumbersome to say 'No' than to say 'Yes' to all Google's data processing. This is a practice considered a 'dark pattern' by the European Data Protection Board and which runs counter to the principle of data protection by design.



8 EDPB Guidelines, 'Dark Patterns in Social Media Platform Interfaces: How to recognise and avoid them' (March 2022) section 4.4.2, page 52.

Moving beyond this first step, no matter the option chosen by the consumer – 'Express' or 'Manual' – the language Google uses at every step of the registration process regarding the different settings is unclear, incomplete, and misleading. For example, as illustrated below, important information about data processing 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 option as one where consumers will miss out on advantages if they don't consent to Google's extensive tracking and profiling practices.

In summary, through a combination of deceptive design, unclear language, misleading choices and missing information, Google's account sign-up process is deliberately steering consumers to allow an extensive and invasive processing of their personal data. Instead of 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, Google is steering people towards its surveillance system where everything they do is monitored and exploited by the digital behemoth.



This setting is about much more than ‘faster searching’.

There are other possible retention periods e.g. three months, which are not communicated up front, and which can only be selected once an account has been created.

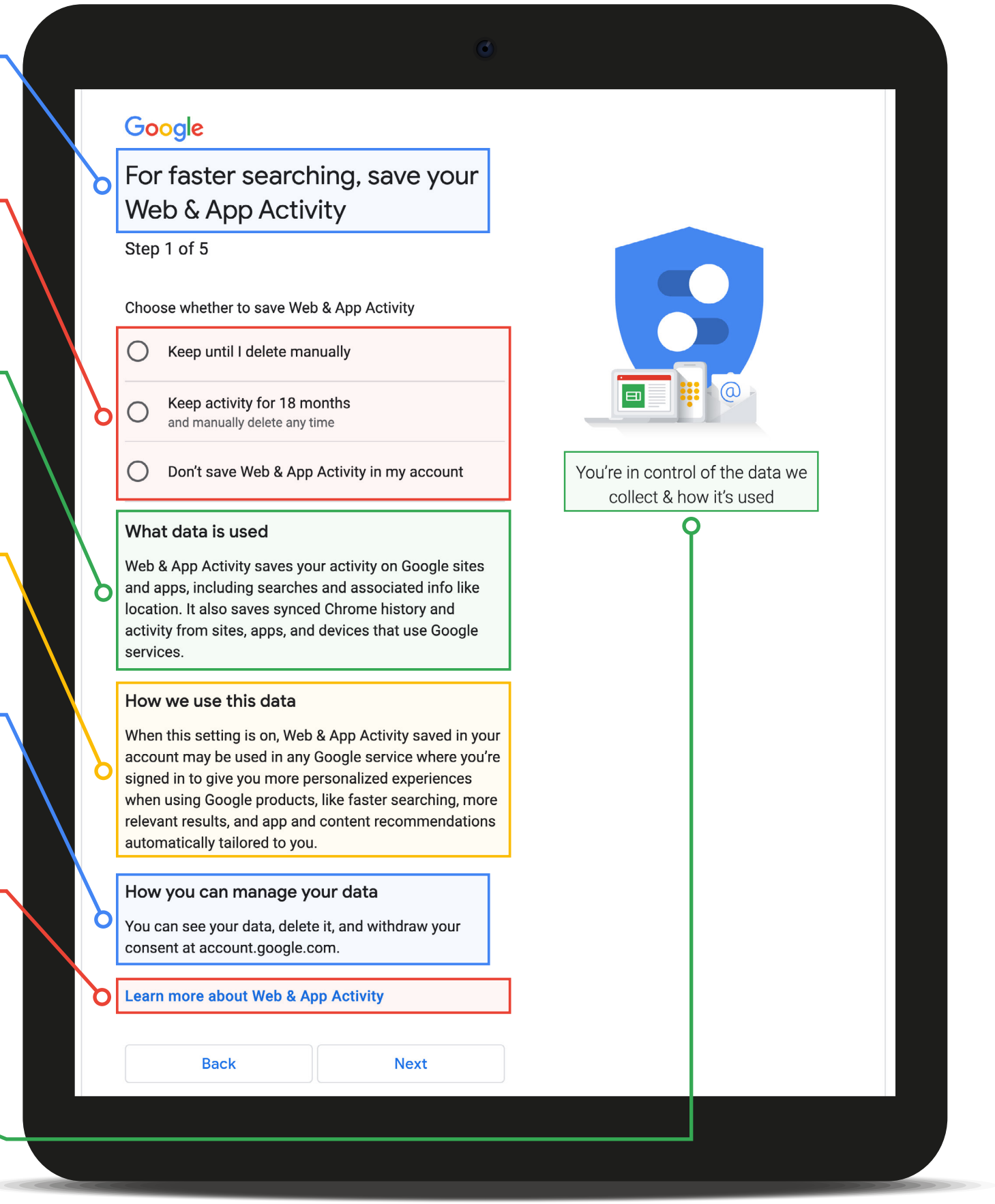
Very extensive, excessive, and invasive data collection, covering much more than what the user can reasonably expect and would seem necessary for the stated purposes.

The use of personal data for advertising purposes is not mentioned at all. The stated purposes are rather vague and generic. There is no mention of the legal basis used for processing.

Regarding withdrawal of consent, once an account is opened, it is only possible to ‘pause’ Web & App activity.

Important information about the purposes of processing is only available after clicking here e.g. regarding ad personalisation. But the additional info still leaves users in the dark about the purposes for the processing and the legal bases which Google relies on.

Users cannot really know what this setting entails in terms of data processing, plus it bundles a lot of different purposes and processing operations the user has no granular control of.


Google
For faster searching, save your Web & App Activity
Step 1 of 5
Choose whether to save Web & App Activity
Keep until I delete manually
Keep activity for 18 months
and manually delete any time
Don't save Web & App Activity in my account
What data is used
Web & App Activity saves your activity on Google sites and apps, including searches and associated info like location. It also saves synced Chrome history and activity from sites, apps, and devices that use Google services.
How we use this data
When this setting is on, Web & App Activity saved in your account may be used in any Google service where you're signed in to give you more personalized experiences when using Google products, like faster searching, more relevant results, and app and content recommendations automatically tailored to you.
How you can manage your data
You can see your data, delete it, and withdraw your consent at account.google.com.
Learn more about Web & App Activity
Back
Next
You're in control of the data we collect & how it's used

3 GDPR legal analysis

A legal analysis carried out by BEUC and AWO concludes that the signup process, and the processing of personal data that Google engaged in as a result of it, runs contrary to the EU General Data Protection Regulation (GDPR)[9] in different ways:

- Google relies on consent as a legal basis for some processing, but no valid consent to that processing is collected (Articles 5(1)(a), 6 and 7 GDPR) nor does Google have an alternative valid legal basis for its processing (Articles 5(1)(a) and 6 GDPR).
- Google's processing of personal data is not fair, because the design elements during and after signup seek to influence and/or cause the data subject to agree to more processing of personal data than he otherwise would have (Article 5(1)(a)).
- Google's processing of personal data is not transparent (Articles 5(1)(a), 12 and 13 GDPR).
- Google processes personal data for purposes that are not specified and explicit at the time it is collected, in breach of the purpose limitation principle and transparency obligations (Articles 5(1)(b) and 13(1)(c) GDPR).
- Google processes more data than necessary, and retains it for longer than necessary, in breach of the principles of data minimisation and storage limitation (Articles 5(1)(c) and (e)).
- The overall design of Google's signup process and account settings and the impact they have (lack of clarity and a tendency towards more extensive processing) are inconsistent with 'data protection by design and by default' (Article 25 GDPR).

> **Google processes more personal data and retains it for longer than necessary.**

9 Regulation (EU) 2016/679).

4 **Our requests**: making 'privacy' the default and easiest choice

The consumer organisations involved in this coordinated action request that the competent data protection authorities (DPAs) fully investigate Google's practices, using all their powers under the GDPR, to determine whether Google's processing of account holders' personal data is lawful. Google must stop any unlawful processing operations related to the use of personal data, notably those operations related to the use of such data for advertising purposes.

It must also design and implement a compliant signup process that has privacy by design at the core and provides meaningful transparency to users about how their data will be processed, providing them with a meaningful choice over the range of purposes and services for which Google seeks to process their personal data. DPAs should impose an effective, proportionate, and deterrent fine against Google for any infringements of the GDPR.

Google's Privacy Policy states that *'when you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.'* It prominently tells consumers during the account signup process that they are in control of the data that Google collects and how it is used. In fact, it is rather the opposite.

Google is a dominant force in the 'surveillance economy' and already a repeat offender when it comes to respecting EU data protection and privacy rules.[10] Moreover, various GDPR complaints[11] and court cases[12] against the company are still pending in different jurisdictions. We consider this case to be 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 statement it adopted in Vienna at the end of April.

DPAs must ensure that Google truly puts consumers in control of their personal data and respects their privacy. The starting point must be to make 'privacy' the default and easiest choice when setting up a Google account.

For more detailed information on the legal analysis and requests to DPAs, please see the full GDPR complaint.

---

10 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 on 31 December 2021 against the company over the inability to allow YouTube users in France to refuse cookies as easily as they could accept them.

11 For example, on 4 July 2021, noyb, filed a complaint to the CNIL in France regarding Google's Android Advertising Identifier (AAID). The complaint is still under investigation.

12 For example, 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.

60 YEARS YOUNG
YEARS STRONG

BEUC The European Consumer Organisation

Co-funded by
the European Union