BEUC The European Consumer Organisation

The Consumer Voice in Europe

THE LONG AND WINDING ROAD

Two years of the GDPR: A cross-border data protection enforcement case from a consumer perspective

Contact: David Martin – digital@beuc.eu

Bureau Européen des Unions de Consommateurs AISBL | Der EuropÄische Verbraucherverband
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2020-074 - 05/08/2020

EXECUTIVE SUMMARY

On 25 May 2020, the General Data Protection Regulation (GDPR) celebrated its second anniversary. The GDPR is the main framework for protecting European consumers' privacy and personal data in the digital era. It created an innovative enforcement system for tackling EU-wide data protection infringements by establishing mechanisms for cooperation between national data protection authorities and the consistent application of the rules. The new enforcement system is meant to improve the functioning of the Internal Market as it gives businesses in the EU the possibility to interact with one single authority ("one-stop-shop mechanism", hereafter "OSS") and at the same time aims at increasing effective protection of individuals.

Consumer organisations have high expectations for this new enforcement system to ensure an effective application of the GDPR. Only this will bring fundamental change to a digital economy where widespread commercial surveillance has become a major concern.

In November 2018, BEUC started coordinating the efforts of seven of its member organisations[1] who decided to take action against Google's location tracking practices. Building on the findings of the "Every step you take" report, published by the Norwegian consumer organisation Forbrukerrådet, **BEUC members filed complaints against Google for breaching the GDPR**. Given the cross-border nature of Google's activities, these complaints – originally lodged by our members with their respective national Data Protection Authorities – are now investigated by the Irish Data Protection Commission (DPC) in application of the GDPR's one-stop-shop mechanism ("OSS mechanism"). Over a year and a half after the complaints were lodged, our member organisations are still waiting for a decision.

Based on BEUC member's experience, and following up on our recent recommendations and the European Commission and EDPB assessments of the application of the GDPR, this report reflects the experience acquired of the functioning of the GDPR enforcement system from the standpoint of consumers and national consumer organisations. It illustrates the current lack of effectiveness in the application of the GDPR. In particular, our case illustrates that the lack of harmonised binding administrative procedures to deal with cross-border complaints and the slow pace of proceedings have a negative impact on the protection of millions of consumers across Europe.

We underline that this is the first GDPR case in which BEUC and our members have experienced the functioning of the OSS mechanism. Our complaints involve one of the biggest companies in the world and are being handled by the Irish DPC, who is in charge of several other pending GDPR complaints involving tech giants headquartered in their country. In addition to our experience, other NGOs who brought GDPR complaints have also documented the difficulties they have encountered[2].

[1] Forbrukerrådet (Norway), Consumentenbond (The Netherlands), Ekpizo (Greece), dTest (Czech Republic), Zveza Potrošnikov Slovenije (Slovenia), Sveriges Konsumenter (Sweden) and ForbrugerrådetTænk (Denmark)
[2] https://noyb.eu/en/open-letter

OUR FINDINGS

DECISIONS TAKE TOO LONG WHILST INFRINGEMENTS CONTINUE

Our members lodged their complaints in **November 2018** with their respective national data protection authorities (DPAs). It took nine months, until **July 2019**, before the Irish DPC was appointed lead authority for the complaints. It took another six months, until **February 2020**, for the DPC to announce the opening of an own volition inquiry into the matters raised in our members' complaints[3], and by doing so, initiating a new procedure[4] on top of the one that was already ongoing. This means that at the time of writing this report, over a year and a half after the complaints were launched, a decision on the complaints is still far off and it is unclear when such a decision could be expected. Meanwhile, Google continues to spy on the comings and goings of millions of European consumers. Moreover, since the complaints were launched, the company has even carried out a (misleading) public PR campaign[5] to portray itself as company that respects privacy and highlight that users are in control of their personal data.

LACK OF HARMONISED RULES ON THE REPRESENTATION OF DATA SUBJECTS AND THE ADMISSIBILITY OF COMPLAINTS CREATES LEGAL UNCERTAINTY AND DELAYS

Over a year after the complaints were lodged, the lead authority reached out to BEUC's members requesting evidence that they fulfilled the requirements to represent data subjects under Article 80 GDPR, as well as information to determine the legal interest of the data subjects they represented to lodge the complaints. These requests by the DPC slightly differed from one complaint and country to another complaint and country as per timing and content. This additional information was requested by the lead authority in application of its national law, even though the organisations had presumably already passed through an eligibility screening by their national authorities when the complaints were initially filed. This means that, for cross-border inquiries under the OSS mechanism, data subjects and the organisations representing them must go through a double screening to check that their complaints meet the legal requirements to be admissible. The second (and supposedly decisive) screening is subject to the law of the country of the lead authority, not the national law of the complainants or the organisations in question. All this increases the length of the procedure and could lead to contradictory assessments on the admissibility of the complaints.

LACK OF BINDING HARMONISED PROCEDURAL LAWS, COUPLED WITH THE MAIN ESTABLISHMENT CRITERION TO DETERMINE LEAD SUPERVISORY AUTHORITY, FAVOURS BUSINESSES

In our members' case, the Irish DPC has been appointed as lead authority for dealing with the complaints filed by BEUC's members because the main EU establishment of Google for GDPR purposes is in Ireland. Given that the GDPR does not harmonise national administrative procedural laws, this effectively means that the law applicable for the handling of the complaints is mainly the national of the lead DPA (Irish procedural law). Our members and the complainants they represent are thus subject to laws they are not familiar with. In addition to the admissibility issues outlined above, this naturally works in favour of businesses, who benefit from easier access to justice. Companies will be dealing with their own national DPA, in their own language, will be familiar with their own national procedural laws and will have easy access to lawyers in their country.

[3] https://dataprotection.ie/en/data-protection-commission-launches-statutory-inquiry-googles-processing-location-data-and
[4] Irish DPC - Annual Report 2018 - See page 30 "Phases of a Statutory Inquiry"
[5] https://twitter.com/airavn/status/1199695667083595776?s=20

OWN VOLITION INQUIRY BY THE LEAD AUTHORITY CREATES UNCERTAINTY REGARDING COMPLAINT HANDLING AND COULD UNDERMINE INDIVIDUALS' RIGHTS

The Irish DPC informed our members in February 2020 that it had decided to start an own volition inquiry that "*is likely to inform"* its handling of their complaints. This decision to launch an own volition inquiry raised our concerns regarding the impact on the investigation of the complaints and the exercise of the complainants' rights. The approach taken by the DPC raised questions on the implications of having two distinct yet seemingly interlinked ongoing procedures, one of which our members are a part of (the investigation on the complaints) and one of which in principle they are not (the own volition inquiry) and thus have unclear procedural rights. Also, the DPC's own volition inquiry will investigate Google's business practices as of February 2020 and not from the moment when the complaints were filed, back in November 2018.

OUR RECOMMENDATIONS

In order to address the problems we have identified, BEUC recommends to act swiftly to ensure the effective enforcement of the GDPR and strengthen the position of data subjects and their representing organisations in the framework of cross-border enforcement cases.

In particular, BEUC recommends:

1) The European Data Protection Board (EDPB) to establish the basic elements of a common administrative procedure to handle complaints in cross-border cases under the cooperation mechanism of the GDPR (Article 60).
2) DPAs to ensure that the exercise of their discretionary powers to carry out own-initiative investigations does not in any way undermine the rights of the complainants and/or result in delays.
3) DPAs to thoroughly take up their assistance function when dealing with cross-border complaints.
4) Member States to establish specific support for data subjects, or organisations representing them, involved in cross-border complaints.
5) DPAs –in particular those acting as lead authorities –to fully use their corrective powers under Article 58 GDPR.
6) National DPAs and the EDPB to establish a list of organisations per Member State which should be considered eligible to represent data subjects under Article 80 GDPR. Once considered as such, the principle of mutual recognition should apply so that they could represent data subjects in all EU countries.
7) Member States to implement Article 80 (2) GDPR in their national law to ensure that eligible organisations have the right to lodge complaints without a mandate from a data subject.
8) Member States to ensure that DPAs are sufficiently equipped and have enough resources to perform their tasks.

Table of Contents

1. Our motivation: Putting the GDPR to use in fighting Google's commercial surveillance

Google LCC ("Google") is a subsidiary of Alphabet Inc. It delivers a vast amount of consumer services, including Google Search, Google Maps, Gmail, YouTube, and Google Assistant. It also runs a large number of business-facing services, including analytics and advertising services.

Google collects the location data of consumers for different purposes and a large variety of its services, including by tracking their smartphones and connected devices. Geolocation data is part of a bigger picture and can be combined with other data such as internet browsing history, preferences, social media activities, online shopping history, etc. In other words, through its various services, Google can create a very comprehensive picture of its users.

Location tracking can have advantages: faster mobility, simplification of purchases, service improvements, etc. However, our movements tell a lot about us. The places we frequent can reveal many things about ourselves. For example, religious views (went to a place of worship), political stance (attended a protest march), and health related issues (visited a cancer treatment centre). This can be used for many purposes, including to target advertising, or for individualised offers and services, using the information acquired to influence the individual.

The report "Every step you take", published by BEUC's Norwegian member Forbrukerrådet in November 2018 showed how extensively Google's data location tracking endangers consumers' privacy and how the company uses deceiving techniques to push users into making privacy-intrusive and non-informed choices for the company's own benefit and control.

Google provides most of its consumer-facing services at no direct financial cost to the user. Rather than having users pay a monetary fee for using its services, Google collects vast amounts of users' data and monetises it through advertising and other business-facing services. This type of "surveillance-based'' business model has unfortunately become widespread in the digital economy, creating major concerns from a consumer privacy and autonomy standpoint as technology is designed and used to capture and control human behaviour.

The GDPR, applicable since May 2018, is considered a 'pioneering' law, setting a global standard for data protection and providing the tools to fight back against online commercial surveillance and surveillance capitalism[6].

One of the main novelties introduced by the GDPR is its new enforcement system. With its cooperation and consistency mechanism at the core, this new system has generated high expectations among consumer organisations and privacy advocates. It is designed to tackle EU-wide infringements and ensure a coordinated and consistent application of the rules. It aims to respond to the needs of the Internal Market and thus avoid administrative burden for business, but also to provide consumers across the EU with the effective protection they need.

In this context, and based on Forbrukerrådet's research, in November 2018 seven BEUC members asked their national Data Protection Authorities to act in defense of consumers

[6] https://en.wikipedia.org/wiki/Surveillance_capitalism

and ascertain numerous violations of the GDPR by Google with regards to the company's location tracking practices[7].

2. Our coordinated action: "Every Step You Take"

2.1. BEUC as coordinator of consumer organisations enforcement actions

BEUC represents 44 independent consumer organisations from 32 European countries. One of our activities is to coordinate enforcement actions undertaken by our members when a trader's illegal practice(s) have an EU dimension. Such co-ordinated initiatives are necessary because enforcement measures in most sectors are still confined to the territorial jurisdiction of Member States. Despite of the fact that we have a Single Market since 1992, the EU today has not yet advanced in establishing a "Single Enforcement Area". Our goal with these co-ordinated initiatives is to stop illegal business practices affecting consumers EU-wide in the most efficient way possible.

After many years focusing on consumer law enforcement[8], the GDPR and its new enforcement tools has led BEUC to take up the challenge of co-ordinating consumer organisations' activities in the area of data protection enforcement.

The case analysed in this report is our first co-ordinated GDPR action. It particularly involves seven of our members[9] who, on behalf of individual consumers, filed a series of complaints against Google before their respective national DPAs. These complaints concern how the company tracks its users' location.

BEUC's role is to coordinate the activities of the members involved in the case. We provide the platform for them to exchange about progress, share information received from their national DPAs and agree on a course of action. In our role as coordinator we also interact with the Irish Data Protection Commission, who is the DPA in charge of investigating our members' complaints as lead authority under the GDPR One-Stop-Shop Mechanism. In addition, as EU representative for our members, we are in contact with the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), the European Commission and the Consumer Protection Cooperation Network (CPC) to inform them about key developments.

2.2. "Every Step You Take": legal analysis, complaints and requests to DPAs

Starting from a technical and commercial analysis of Google's Android operating system – to be considered by far the dominant operating system with an estimated 85% of the global mobile market share – the "Every Step You Take" report showed how Google is able to collect and process users' data using deceptive techniques and user interface design tricks (so called "dark patterns"). It also explained how such practices are incompatible with the GDPR.

Google collects users' location through the settings "Location history" and "Web & App activity", present in every Google account. The processing of these personal data is only lawful if Google relies on one of the six legal bases mentioned in Article 6 of the GDPR[10]. Therefore, when assessing compliance with the GDPR, the first step is to determine which

[7] https://www.beuc.eu/publications/consumer-groups-across-europe-file-complaints-against-google-breach-gdpr/html
[8] https://www.beuc.eu/press-media/news-events/new-report-suggests-ways-improve-enforcement-consumer-rights
[9] Forbrukerrådet (Norway), Consumentenbond (The Netherlands), Ekpizo (Greece), dTest (Czech Republic), Zveza Potrošnikov Slovenije (Slovenia), Sveriges Konsumenter (Sweden) and ForbrugerrådetTænk (Denmark).
[10] Consent, performance of a contract, legal obligation, public interest, vital interest of the data subject, legitimate interests.

legal basis is used and for which purpose. In this case, the legal and technical analysis showed that Google lacked a lawful legal ground for processing the location data in question.

First of all, Google did not provide clear information to users regarding which legal grounds it applies to which processing operations, as required by the transparency principle and obligations imposed by the GDPR[11]. Transparent processing is about being clear, open and honest with data subjects about who, how, when and for what purposes their personal data is being processed[12]. GDPR obliges companies to provide consumers with information in a way that is easily accessible, easy to understand and therefore in plain language. In this case, relevant information was often incomplete, unclear, hidden in sub-menus or scattered across different sections. The consumer was forced to juggle through various levels and clicks before reaching important information. In this way it is almost impossible for consumers to understand what is happening with their personal data.

Furthermore, the analysis of the legal bases seemingly used by Google showed that they did not meet the conditions to be considered valid for the data processing in question.

Location History

Google seemingly relied on consent[13] as the legal basis for processing location data for all purposes related to the Location History feature, given that this feature depended on users opting-in. However, such a consent could not be considered legally valid under the GDPR as it was not:

- Freely given: Users were guided through processes that basically compelled them to consent to the processing of their location data, simply by following the click-flow. Also, enabling Location History was required in order to enable other services such as Google Assistant.
- Specific: Google provided users with blurred information on the purposes of processing activities. The main purpose to "provide more personalised experiences" is not specific enough. Other mentioned purposes (e.g. to create a map, to show relevant advertising on and off Google) were presented as a 'non-exhaustive' list of examples of 'personalisation', rather than separate purposes.
- Informed: Most of the times, important information about the purposes of the processing and the users' choices was hidden behind extra clicks and sub-menus.
- Unambiguous: Due to Android's deceptive design, it was not clear to users that they were actually giving consent to something, and even if it was, to what exactly they were consenting to.

Web & App Activity

With regards to the Web & App Activity feature, things were even less clear. If Google relied on consent for the purposes embedded in this feature, the fact that Web & Activity was turned on by default would immediately mean that Google was 'forcing' users to consent and therefore this consent is not valid. Otherwise, Google relied on a different legal ground for processing, namely legitimate interests[14], which would be inadequate due to the significant impact of the data processing in question on the rights and freedoms of the individual.

[11] Article 5.1(a) and Articles 12-14 GDPR
[12] WP29/EDPB Guidelines on Transparency under Regulation 2016/679 https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025
[13] Article 6(1)(a) and Article 7 GDPR
[14] Article 6(1)(f) GDPR

Complaints and requests to DPAs

Following these findings, seven of our members filed formal complaints[15] on behalf of individual data subjects under Art. 80 (1) GDPR. DPAs were requested to investigate and determine:

- Whether Google had a lawful legal basis to process the complainants' location data, particularly for those purposes related to advertising; and whether Google was properly informing the complainants about which legal basis the company used to process their location data and for which purposes it was doing so.
- Whether the conditions set out in Article 7 of the GDPR for valid consent were met, notably in those cases where Google may rely on consent as a legal basis for processing location data for advertising purposes.
- Whether 'legitimate interests' constituted an appropriate legal basis for the processing of location data carried out by Google in the context of the processing operations addressed by the complaints, notably in relation to advertising purposes.
- Whether the design patterns and tricks used by Google to push users to share location data are compatible with the principles set forth in Articles 5.1 (a) and Article 25 of the GDPR regarding the fairness and transparency of processing and data protection by design and by default.

DPAs were also asked to:

- Require Google to stop any unlawful processing operations related to the use of location data, notably those operations related to the use of such data for advertising purposes.
- Impose an effective, proportionate and deterrent fine against Google for the infringements of the GDPR, considering:
    - The number of users affected beyond the complainants (potentially anyone with an Android phone and/or a Google account).
    - That Google is a 'repeat offender' in terms of data protection law infringements.
    - The sensitivity of location data.
    - The financial gains that Google takes from processing personal data for advertising purposes and the dominant market power of the company.
    - That fundamental principles of the GDPR, as well as provisions related to the data subjects' rights, have been infringed.

3. General overview of our members' experiences so far

The BEUC member organisations involved in this coordinated action have experienced slightly different handlings of their complaints. This can create uncertainty about the rules and procedures to handle complaints, which ultimately weighs down on the individuals and the organisations representing them.

Below is a general overview of our members' experiences so far, focusing on key formal interactions between our members and the DPAs. The BEUC Secretariat and Forbrukerrådet

[15] https://fil.forbrukerradet.no/wp-content/uploads/2018/11/complaint-google-27-november-2018.pdf

also met the Irish DPC in Dublin at the end of January 2020 to discuss the state of play on the complaints.

3.1. Forbrukerrådet (Norway)

Forbrukerrådet filed a complaint to the Norwegian DPA on 27 November 2018. In late July 2019, the Norwegian DPA informed them that the Irish DPC had been appointed as the lead authority. In November 2019, the Irish DPC, via the Norwegian DPA, asked them for additional information regarding their capability to represent a data subject under Art. 80 (1) GDPR. Shortly after, the Irish DPC requested them to provide additional information about the data subject they represented. Forbrukerrådet asked the DPC to refine its request, as some aspects were considered disproportionate by the data subject. In the end the DPC considered Forbrukerrådet had provided all the necessary information. Prior to that, in February 2020, the DPC had informed Forbrukerrådet about the progress in the investigation of the complaint and the opening of the DPC's own volition inquiry into Google's practices.

3.2. Sveriges Konsumenter (Sweden)

The data subject represented by Sveriges Konsumenter (SK) filed its complaint to the Swedish DPA on 27 November 2018. Differently from the rest of the organisations, the complaint was *not* filed by SK on behalf of the complainant but by the complainant directly, since Swedish administrative law makes it impossible for an organisation to represent an individual in legal matters. Between January and April 2019, the Swedish DPA investigated the complaint and had various exchanges with both SK and Google, including formal requests for information submitted to the company. In August 2019, the Swedish DPA officially informed SK that the complaint had been transferred to the Irish DPC[16].

3.3. Consumentenbond (Netherlands)

Consumentenbond (CB) filed a complaint to the Dutch DPA on 26 November 2018. In parallel, CB sent a formal enforcement request to the DPA using their legal status under Dutch law. Before being informed by the DPA at the beginning of June 2019 that the Irish DPC would be appointed the lead authority, CB attempted to urge the Dutch authority to investigate on the matter, including through a petition with more than 50,000 signatories subscribing the concerns raised in the complaint. In December 2019, the Irish DPC, requested CB via the Dutch DPA to provide more information on the data subject they represented. In February 2020, via the Dutch Authority, the DPC informed CB on the progress of the complaint and the opening of its own volition inquiry into Google's practices.

3.4. EKPIZO (Greece)

EKPIZO filed a complaint to the Greek DPA on 20 December 2018. In June 2019, EKPIZO was informed by the Greek DPA that the Irish DPC would become the lead authority. In late November 2019, via the Greek DPA, the Irish DPA requested EKPIZO to provide information about its capability to represent a data subject under Article 80(1) GDPR, as well as about how the alleged infringements affected the data subject they represented. In March 2020, via the Greek DPA, the Irish DPC informed EKPIZO about the progress of the complaint and the opening of its own volition inquiry into Google's practices.

3.5. Zveza Potrošnikov Slovenije (Slovenia)

Zveza Potrošnikov Slovenije (ZPS) filed a complaint to the Slovenian DPA on 27 November 2018. In November 2019, via the Slovenian DPA, the Irish DPC asked ZPS to provide

[16] Official press release in Swedish

information about its capability to represent a data subject under Article 80(1) of the GDPR. The DPC also requested evidence on how the alleged infringements of the GDPR affected the complainant. In March 2020, via the Slovenian DPA, the Irish DPC informed ZPS about the progress of the complaint and the opening of its own volition inquiry into Google's practices.

3.6. dTest (Czech Republic)

dTest filed the complaint to the Czech DPA on 11 December 2018. In January 2019, the Czech DPA asked dTest to provide the mandate by the complainant. dTest received another letter from the Czech DPA in late July 2019 informing them that there were no updates from the lead authority (Irish DPC). In March 2020, via the Czech DPA, dTest received two requests from the Irish DPC to provide more information regarding its capability to represent a data subject under Article 80 (1) GDPR and how the alleged infringements affected the complainant. Later in March 2020, the DPC, again via the Czech DPA, informed dTest about the progress of the complaint and the opening of its own volition inquiry into Google's practices.

3.7. Forbrugerrådet Tænk (Denmark)

Forbrugerrådet Tænk had already submitted a separate complaint on Google's handling of location data to the Danish DPA back in March 2018. They sent a letter to the authority following up on the complaint to the DPA when the "Every Step You Take'' report was published, and the other BEUC members submitted their complaints in November 2018. Some months later, they were requested to re-submit their complaint on behalf of a data subject, pursuant to Article 80(1) of the GDPR. They did so in April 2019 and their complaint has been transferred to the Irish DPC.

4. Considerations regarding the functioning of the one-stop-shop mechanism and GDPR enforcement from a consumer perspective

4.1. A long wait for the appointment of the lead authority

Among the main changes introduced by the GDPR to deal with cross-border enforcement cases are the OSS mechanism and the cooperation and consistency mechanisms[17].

The OSS mechanism is used to determine which DPA should take the lead in an investigation involving multiple DPAs. The 'lead authority' is determined by the location of the main establishment of the company subject to investigation. What should be considered as the main establishment is defined in Article 4 (16) GDPR[18].

According to the criteria set out by the GDPR, Google's main EU establishment is considered to be in Ireland. This has led to the appointment of the Irish DPC as lead authority for the investigation of the complaints filed by BEUC members.

[17] One-Stop-Shop mechanism, Articles 56-60 GDPR. Cooperation and consistency mechanism, Chapter VI GDPR.

[18] With regard to a controller with establishments in more than one Member State as in the case of Google, "main establishment" means "*the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment*". Furthermore, Recital 22 GDPR clarifies that an "*establishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect*".

The appointment of the Irish DPC as lead authority was officially communicated to our members in July 2019, long after the first complaints were lodged back in November 2018. The appointment process might have taken longer than usual because Google did not officially set its main establishment for GDPR purposes in Ireland until late January 2019. However, it still took several months after that for the DPC to be appointed, even if – as early as February 2019 – it became clear that the case would go to Ireland.

4.2. The representation of data subjects and the admissibility of the complaints

In order to strengthen and facilitate the protection of data subjects' rights, the GDPR allows individuals to mandate an organisation to act on their behalf to lodge a complaint with a supervisory authority. The conditions that need to be met by the organisation and the actions it can undertake are set out in Article 80 (1) GDPR. Namely, the organisation must:

- be *"properly constituted in accordance with the law of a Member State"*
- have *"statutory objectives which are in the public interest"*
- be *"active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data (..)".*

All BEUC members that lodged complaints did so under Article 80 (1), except our Swedish member. None of the DPAs that received the complaints questioned the legal standing of our members to represent data subjects or the admissibility of the complaints. In the months following the filing of the complaints, the concerned DPAs informed our members about the developments with regards to the handling of their complaints and, finally, of the appointment of the Irish DPC as lead authority. All this would indicate that the concerned DPAs considered our members to meet the conditions to represent data subjects and that the complaints were admissible.

Nonetheless, upon taking charge of the procedure, the DPC checked the standing of our members and the admissibility of the complaints (again) under its own national law. For example, in November 2019 (one year after their initial complaint was filed), the DPC asked our Norwegian member to provide documentation about its proper constitution to demonstrate it meets all criteria set out in Article 80 GDPR. Our members also received requests to provide additional information about the complainants they represented and how they were affected by the alleged infringements, including information about their Google accounts and requests for evidence like screenshots that documented they experienced the issues raised in the complaints.

All these additional requests of information and admissibility checks after the appointment of the lead authority and so long after complaints were initially filed raise questions as to the efficiency and consistency of the administrative procedures to handle cross-border complaints. Moreover, it further delays the investigation of the substance of the complaints and increases the length of the procedure. It also puts additional burden on the complainants' side, eventually requiring them to demonstrate the admissibility of their complaints twice, even requesting them to provide detailed evidence such as screenshots.

Moreover, concerns arose in relation to the possibility for organisations to lodge a complaint independently of a data subject's mandate, as envisaged in Article 80 (2) GDPR. According to this Article, it is up to the Member States to allow or not for this to be possible. For example, Dutch law provides for this possibility and in this case our Dutch member has brought a complaint on its own, in addition to the complaint brought on behalf of an individual consumer. However, Irish law does not provide for this possibility and the Irish DPC has clearly told our members that a complaint without a mandate would not be admissible. For example, our Danish member had to turn their initial complaint into a complaint on behalf of a data subject. This creates a further impasse and uncertainty which to date seems unsolved. It is important to have clarity about which law prevails should a

complaint under Article 80 (2) in a country where this article has been implemented end up being transferred to a country where this has not been the case.

The right to representation is crucial for achieving the goal of the GDPR to strengthen the protection of data subject rights. It is thus regrettable that the GDPR leaves a regulatory choice about non-mandated representation to the Member States and that only a few have allowed for such representation. It is not possible to achieve effective protection of data subjects in practice if the modalities under which their right to representation is to be exercised are not harmonised and equally available to all EU data subjects.

4.3. The Irish DPC's own volition inquiry

More than one year after the complaints were filed, on 4 February 2020, the Irish DPC announced the opening of an own volition statutory inquiry pursuant to Section 110 of the Irish Data Protection Act.

According to the announcement[19] by the Irish DPC, the inquiry will set out to establish whether Google has a valid legal basis for processing the location data of its users and whether it meets its obligations as a data controller with regard to transparency. The DPC told our members that the inquiry "*is likely to inform*" the handling of their complaints.

The decision to carry out such an inquiry at this stage raised important questions and concerns regarding the effective handling of the complaints and the respect of the rights of the complainants. In particular, our concerns related to the timeframe covered by the investigation, which will only look into Google's practices from the moment the inquiry was opened (February 2020) and not from the date where the initial complaints were filed (November 2018); the risk of further delays in the adoption of a decision on the complaints, given that the inquiry represents an additional new procedure on its own[20] that will take place before a decision is taken on the complaints; the complainants' right to be heard, since they are not formally a party in the own volition inquiry; and their right (or not) to appeal the Irish DPC's decision on its own volition inquiry.

Due to these concerns, 3 BEUC members involved in the action considered opening a judicial review before the Irish High Court of the DPC's decision to carry out an own volition inquiry. In the end they decided not to proceed, following various exchanges with the DPC to clarify several questions related to the above-mentioned concerns and given the significant legal costs that a judicial review procedure in Ireland would entail.

4.4. An additional obstacle: being subject to foreign law and costs of procedure

Given the absence of harmonised administrative procedures under the GDPR, the law applicable for handling the complaints in a cross-border case under the one-stop-shop mechanism is basically that of the company being subject to investigation. This means data subjects and representative organisations coming from different EU countries are obliged to be subject to laws they do not know.

This ends up favouring the companies under investigation, who would benefit from easier access to justice. Companies will be dealing with their own national DPA, in their own language. They will be familiar with their own national procedural laws and will have easy access to lawyers in their country. For an ordinary consumer it is hardly possible to have access to legal advice in a foreign country, whereas this might be necessary to understand

[19] https://dataprotection.ie/en/data-protection-commission-launches-statutory-inquiry-googles-processing-location-data-and
[20] Irish DPC - Annual Report 2018 - See page 30 "Phases of a Statutory Inquiry"

their procedural rights, the available remedies and the decisions taken by the lead authority. For consumer organisations that represent data subjects, such as BEUC members, access to foreign legal advice and representation in court if needed, is complicated and costly. If the lead authority is in a country with tradition in 'common law', like Ireland, things can become even more complex and costly.

The impact of this situation on the effective application of the GDPR and the exercise of the data subjects' rights should be considered and, initiatives to mitigate this problem should be taken urgently.

4.5. Fighting a moving target

While our members and the respective consumers are still waiting for a decision on their complaints, Google keeps making tweaks to its policies and practices without fundamental changes that would address the problems identified in the complaints.

Since the complaints were launched in November 2018 the company has even carried out a (misleading) public PR campaign[21] to portray itself as company that respects the privacy of its users and highlight that they are the ones in control of their personal data.

20 months after the complaints were filed, we are still far from a decision on whether the company's practices are in breach of the GDPR. Consequently, potential remedies and sanctions have not been put in place and European consumers remain exposed to non-compliant practices. In light of this situation and in an environment where companies become moving targets it is important that DPAs adapt their enforcement approach to intervene more rapidly and directly.

5. Recommendations

Over two years have passed since the GDPR became applicable, we have now reached a turning point. The GDPR must finally show its strength and become a catalyst for urgently needed changes in business practices. Our members experience and that of other civil society organisations, reveals a series of obstacles that significantly hamper the effective application of the GDPR and the correct functioning of its enforcement system.
BEUC recommends to the relevant EU and national authorities to make a **comprehensive and joint effort** to ensure the swift enforcement of the rules and improve the position of data subjects and their representing organisations, particularly in the framework of cross-border enforcement cases.

[21] https://twitter.com/airavn/status/1199695667083595776?s=20

In particular, BEUC recommends[22]:

1) **The European Data Protection Board (EDPB) to establish the basic elements of a common administrative procedure to handle complaints in cross-border cases under the cooperation mechanism of the GDPR (Article 60).**This should be done by urgent guidance of the EDPB and include inter alia common timelines for carrying out investigations and adopting decisions. The EDPB should also provide a uniform interpretation of key GDPR terms such as "without delay", "amicable settlements" and "decision''. In addition, the position of the complainants during the proceedings should be harmonised and made clear in national administrative procedures applicable to DPAs. Complainants should not be limited to have a passive role during the procedure. As a way of example, complainants should be able to intervene at different stages (e.g. when the decision to allocate their complaint to a specific DPA is adopted), not only at the very end when a decision on their complaint is taken. In the longer term, this procedural harmonisation should be done via legislation.
2) **DPAs to ensure that the exercise of their discretionary powers to carry out own-initiative investigations does not in any way undermine the rights of the complainants and/or result in delays**. This should particularly apply when an own-initiative investigation is opened alongside an ongoing complaint procedure in the frame of Article 60 GDPR.
3) **DPAs to thoroughly take up their assistance function when dealing with cross-border complaints.** When acting as concerned DPAs (i.e. not as lead authorities) under the GDPR cooperation mechanism, they should be as proactive as possible to contribute to the investigations of the lead authority. Lead authorities should encourage concerned DPAs to fulfil this task. When relevant, concerned DPAs should not hesitate to use their power to adopt urgency measures under Article 66 GDPR. Also, concerned DPAs should take up an assistance function towards their national data subjects, proactively and regularly advising and communicating with them throughout the complaint handling procedure.
4) **Member States to establish specific support for data subjects, or organisations representing them, involved in cross-border complaints.** In case of cross-border complaints, procedural costs quickly become obstacles to the efficient exercise of data subjects' rights. Thus, measures to limit such costs and support access to legal advice under foreign law, such as access to legal aid, should be put in place.
5) **DPAs –in particular those acting as lead authorities –to fully use their corrective powers under Article 58 GDPR.** This includes adopting interim measures, issuing reprimands and orders and ultimately stopping illegal processing when it significantly affects data subjects.
6) **National DPAs and the EDPB to establish a list of organisations per Member State which should be considered eligible to represent data subjects under Article 80 GDPR.** Such organisations should be considered eligible after a screening by their national supervisory authority. Once considered as such, the principle of **mutual recognition** should apply so that they could represent data subjects in all EU countries.
7) **Member States to implement Article 80.2GDPR in their national law to ensure that eligible organisations have the right to lodge complaints without a mandate from a data subject.** This is necessary to avoid unequal treatment and fragmented protection to fundamental rights across the EU. In the

[22] https://www.beuc.eu/publications/beuc-x-2020-040_gdpr_second_anniversary_-_recommendations_for_efficient_enforcement_letter.pdf

long term, all the rules governing the representation of data subjects should be fully harmonised.

8) **Member States to ensure that DPAs are sufficiently equipped and have enough resources to perform their tasks.** This is clearly required by the GDPR. The Commission should not hesitate to launch infringement procedures if Member States are not meeting their obligations.

6. Conclusions

Two years after its entry into application, the expectations that the GDPR would tackle systemic data protection infringements inherent to the widespread commercial surveillance in our digital world have yet to materialise. The GDPR enforcement architecture is revealing its weaknesses and shortcomings, and this is having a negative impact on the protection of millions of consumers across Europe.

BEUC members' experience with the GDPR one-stop-shop procedure illustrates well the existing concerns which relate among other issues to the lack of harmonised, binding administrative procedures to deal with cross-border complaints; the generally slow pace of proceedings; the lack of resources for DPAs; and the current concentration of important complaints against key tech players in the hands of one single national authority–which has led to an enforcement bottleneck effect.

BEUC and its members are working intensely to make the consumer voice heard. We will continue working to ensure the GDPR is fully enforced and that companies like Google are held accountable for their practices where necessary. Enforcement authorities and Member States must step up to the challenge and fulfil their duties. More efforts are needed to ensure that the GDPR lives up to its global standard status and delivers tangible benefits for individuals and society.

We hope that this report will shed light on the existing problems, help the EU institutions and national authorities to address them quickly and thus make the GDPR an effective instrument to protect people's privacy and personal data.

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).