noyb

European Center
for Digital Rights

Annual Report

2023

noyb.eu

Table of Contents

Preface

noyb continues to be one of the major European forces pushing for the fundamental right to data protection for all users. While the GDPR always foresaw a role for non-profits have in this regard, we see that the lack of enforcement by data protection authorities (DPAs) and little interest by courts makes *noyb*'s work more relevant every year. Above all, we are seeing that the initial "GDPR hype" is now over and that companies have largely learned that the GDPR is not really being enforced and that non-compliance is largely paying off.

While we continued to work on our more than 800 existing cases – many of which are still pending with the authorities– this year we have focused our efforts on filing a number of new complaints against major companies across Europe. This has allowed us to tackle issues such as freely given consent, credit scoring, political microtargeting, profiling & automated decision making and data subject rights.

In total, we filed more than 40 new complaints in various jurisdictions in 2023. Among the most significant cases of 2023 are *noyb*'s first two complaints against Meta's "Pay or Okay" system. In November 2023, the company began charging users a vmonthly fee if they refused to consent to tracking for personalised advertising. *noyb*'s first complaint targets the consent mechanism itself, while the second one focuses on the lack of an easy way to withdraw consent.

But not only that: Among other things, we've also stepped up our action against unlawful credit scoring, filed complaints against twitter (now X) and the EU Commission for the use of political microtargeting X, filed complaints against Fitbit for forced consent, another against Ryanair's use of invasive facial recognition, and one against TeleSign for secretly profiling millions of mobile phone users.

In addition to filing more cases, 2023 was also a year of major decisions in *noyb* cases that resulted in fines against several companies. The year began with the Irish DPC ordering Meta to pay a whopping € 390 million in early January. At the end of May 2023, Meta was fined € 1.2 billion and was ordered to stop transferring Europeans' personal data to the United States.

Then, in June, the Swedish Data Protection Authority (IMY) fined Spotify 58 million Swedish Crown (about € 5 million) because it failed to fully comply with a user's request for access. In the same month, the French data protection authority (CNIL) fined CRITEO, a major online advertising and tracking company in Europe, €40 million for violating data subject rights and failing to prove that it had obtained valid consent. In July, the Swedish data protection authority (IMY) issued the first major fine for the use of Google Analytics. All these fines were the result of complaints that *noyb* (sometimes in cooperation with others) lodged on behalf of data subjects.

We also continued to invest time and effort in expanding our data protection knowledge database GDPRhub. By the end of 2023, it already contained more than 3,000 decisions and judgements from across Europe. This project is made possible by our more than 300 active volunteers, who, together with our team, have helped us build the largest free database of GDPR knowledge. We will continue to expand our knowledge sharing work in 2024, and hope that it will continue to improve compliance among stakeholders who simply need more information about the GDPR and its implementation.

In addition to legal action and technical solutions, we aim to use of PR and media initiatives to highlight and secure the right to privacy. Our team of now twenty people has participated in numerous events such as conferences, summits, hearings and discussions, and has given interviews or published insights in almost every European Member State. We have issued 45 press statements, published hundreds of social media posts on seven different platforms and have managed to be an active voice in the public discourse on privacy and data protection.


PHOTO BY GEORG MOLTERER

None of our work would have been possible without our more than 5,100 supporting members, institutional members and every individual person who has donated to *noyb*. We deeply appreciate this support, especially in these difficult economic times. Your generosity and commitment enables us to continue our work and make a meaningful impact on digital rights.

Going forward, we expect to see a number of decisions in our pending cases, but will continue to build our legal tech initiatives to create enforcement on a larger scale, challenge inactive data protection authorities and, inevitably, continue to file complaints.

As well as focusing on lawsuits against regulators that fail to deal with complaints within a reasonable time, *noyb* will also take direct action against companies, including through collective redress. The Directive on Collective Redress has entered into force in the summer of 2023 and should have already been implemented in the Member States in 2022. While this will be a challenge on an organisational, technical and resource level, we are convinced that collective redress will be an important building block to take action against large-scale wilful violations of the GDPR.

We are excited to see where our journey will lead. I would like to thank the *noyb* team and our supporters for getting us this far in only five years!

Max Schrems
HONORARY CHAIRMAN

About noyb

2.1 Our Mission

noyb follows the idea of targeted and strategic litigation in order to strengthen the right to privacy: In practice, we pursue this goal by thoroughly analysing and prioritising privacy violations, identifying the legal weak spots of these cases and litigating them using the best possible strategy and the most effective method to achieve maximum impact. *noyb* either files complaints against companies with the relevant data protection authority (DPA) or brings cases directly before the courts. Our litigation strategy differentiates between standard-setting cases and enforcement actions.

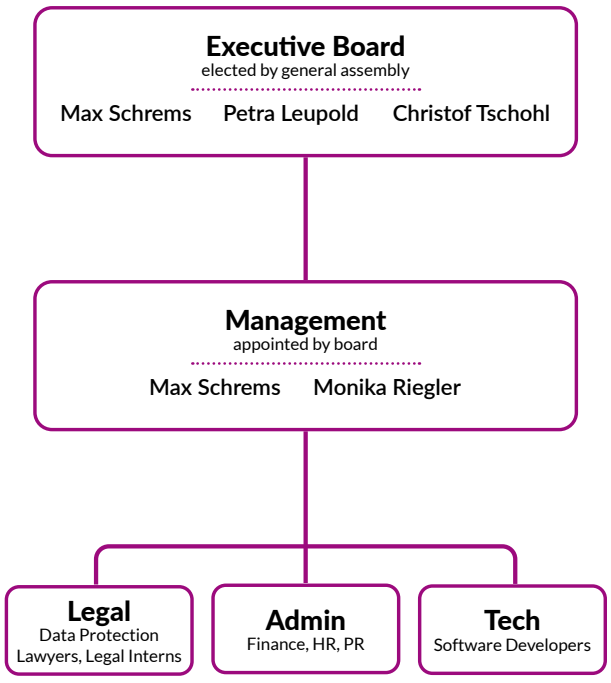
We also use public relations and media initiatives to promote the right to privacy without resorting to litigation. In addition, we promote a common understanding of the GDPR and provide an information platform called GDPRhub, which summarises GDPR decisions and legal literature. Last but not least, *noyb* is joining forces with other organisations to maximise the impact of the GDPR while avoiding parallel structures.

2.2 Who we are

noyb's General Assembly consists of distinguished individual members who are deeply committed to privacy, the GDPR and the enforcement of fundamental rights, as well as representatives of our institutional members such as the City of Vienna, the Austrian Chamber of Labor and others. The General Assembly meets once every two years and appoints the Executive Board.

The Executive Board ("Vorstand") sets the long-term goals, reviews the operations of the organisation and meets once a quarter. According to *noyb*'s Articles of Incorporation, all Board Members serve on a strictly pro bono (volunteer) basis.

The Executive Board can appoint one or more Directors who manage the day-to-day office operations and who may represent *noyb* in any matter. In addition to Max Schrems, who has has been the pro-bono Managing Director at *noyb* since the beginning, Romain Robert has been appointed as Programme Director and has left *noyb* in July 2023. As Operations Director, Monika Riegler is responsible for all administrative matters as well as the PR and IT departments of *noyb*.



Executive Board

Mag. Max Schrems

HONORARY CHAIRMAN & MANAGING DIRECTOR

Max Schrems is an Austrian lawyer, activist and author, who has led a number of successful data protection and privacy cases since 2011. His cases (e.g. on the EU-US Safe-Harbor Agreement) have been widely reported, as enforcement of EU privacy laws has been rare and exceptional. He holds a law degree from the University of Vienna.

We have solid privacy laws in Europe, but we need to collectively enforce them to bring privacy to the living room of users. noyb will work on making privacy a reality for everyone. I am happy to provide my personal experience and network to noyb.

Dr. Petra Leupold, LL.M.

HONORARY BOARD MEMBER

Petra Leupold is the Managing Director of the VKI-Academy, the research academy of the Austrian Consumer Protection Association. She brings invaluable experience in general consumer protection and helps to bridge the gap between the technology and consumer worlds.

Data protection and the right to privacy are core consumer rights. I want to help guide this organization to be a robust advocate for consumer privacy and—as a representative of the Austrian consumer protection agency (VKI) - support it with our longstanding expertise in consumer law enforcement.

Dr. Christof Tschohl.

HONORARY BOARD MEMBER

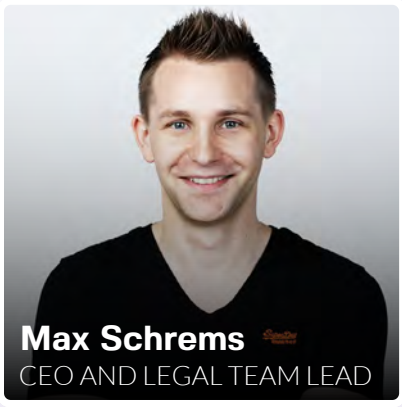
Christof Tschohl successfully overturned the Austrian data retention law and was the chairman of epicenter.works, which is dedicated to defending our rights and freedom on the Internet. Furthermore, he is the scientific director of the Research Institute – Digital Human Rights Center. He holds a Doctorate in Law from the University of Vienna.

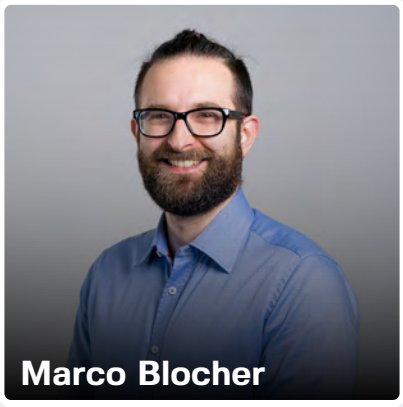
As chairman of 'epicenter.works' I have been working on government surveillance for years. We successfully challenged the EU data retention directive. As a board member of noyb, I am looking forward to closing the enforcement gap in the private sector.

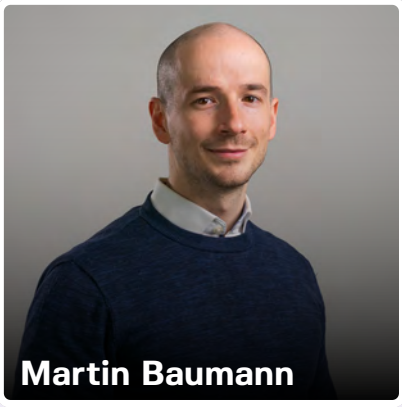
General Assembly

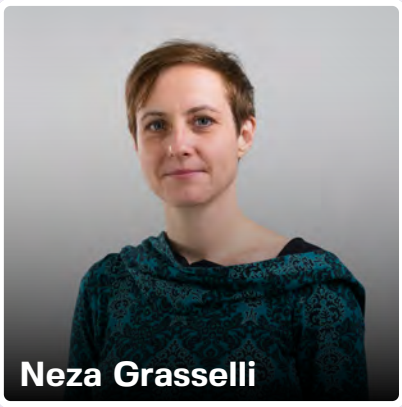
In the course of 2023, we have managed to grow and internationalise our pool of voting members. In addition to our institutional members, the City of Vienna, the Chamber of Labour of Vienna, the Austrian NGO epicenter.works and the German Gesellschaft für Freiheitsrechte, we have 18 voting members from 7 countries. All of them have a strong academic or legal background in the field of data protection, and the GDPR in particular. New members include Shoshana Zuboff (Harvard Professor Emeritus and author of "The Age of Surveillance Capitalism"), Johnny Ryan (ICCL), Katarzyna Szymielewicz (Polish NGO Panoptykon) and the former data protection officers Johannes Caspar and Thilo Weichert.

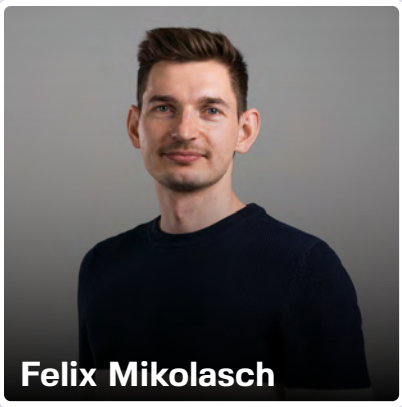
Staff* — Legal Team

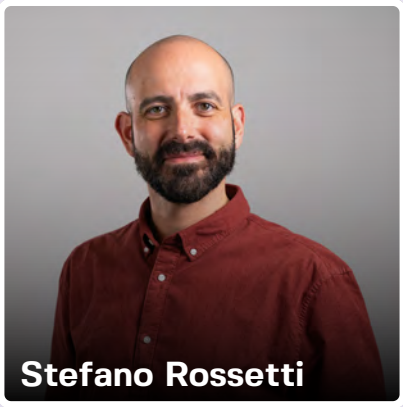










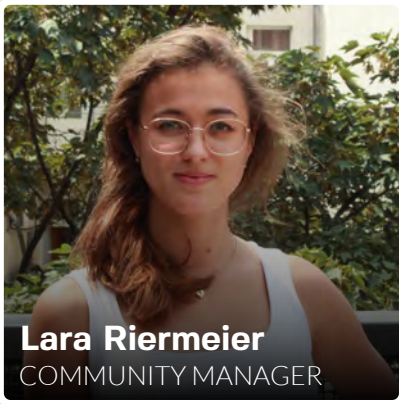


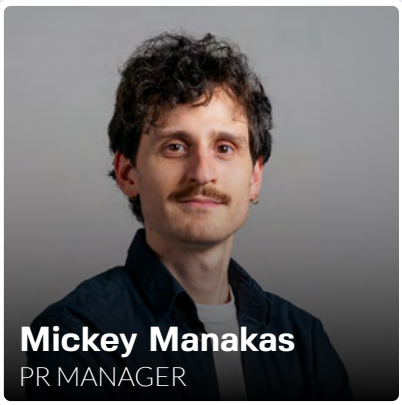
Traineeships

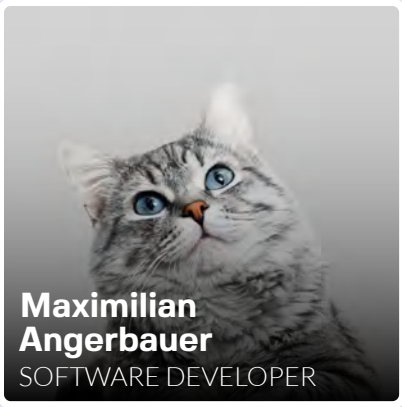
Since October 2018, *noyb* has been offering legal traineeships for university graduates with a strong interest in privacy law. Our trainees gain experience in legal research, factual investigation, and drafting privacy complaints. They also work on *noyb*'s publicly available database, GDPRhub, and *noyb*'s weekly newsletter, GDPRtoday. In 2023, twelve trainees from ten different countries joined *noyb* for a period of three to six months.

**as of December 2023*

Staff* — Office & Tech Team







as of December 2023

2.3 How we work

Many companies ignore Europe's strict privacy laws. They take advantage of the fact that it is often too complicated and expensive for individual users to enforce their fundamental rights, and that any cases brought against companies take a very long time to resolve. When the General Data Protection Regulation (GDPR) came into force in May 2018, it introduced new enforcement mechanisms and ushered in a new era of data protection in the EU. Among other things, Article 80 of the GDPR allows NGOs, such as *noyb*, to represent individual data subjects.

noyb follows the idea of targeted and strategic litigation in order to strengthen the right to privacy: In practice, we pursue this goal by thoroughly analysing and prioritising privacy violations, identifying the legal weak spots of these cases and litigating them with the best possible strategy and the most effective method to achieve maximum impact. *noyb* either files complaints against companies with the competent data protection authority (DPA) or brings cases directly before the courts. Our litigation strategy distinguishes between **standard-setting cases** and **enforcement actions.**

Standard Setting Cases: As the GDPR is a fairly new law, many elements are still unclear or disputed. By developing complex cases targeting these uncertain aspects, *noyb* aims to achieve a decision by the highest courts or privacy bodies in the European Union (CJEU or EDPB) that then will set the standard for future interpretations of the GDPR.

Enforcement Actions: In some cases, the law is very clear, but companies simply don't comply. That's why *noyb*'s enforcement actions don't aim to achieve a decision by the CJEU or the EDPB, but to ensure that national data protection authorities enforce the law on the ground to stop unlawful activities by companies. In order to have an even bigger impact, *noyb* launches mass proceedings and files cases in several countries. Two examples for such enforcement actions are *noyb*'s 101 complaints against unlawful data transfers to the US or our mass complaints against deceptive cookie banners.

2.3.1 Complaints

Complaints are filed with a national data protection authority (DPA). After receiving a complaint, the authority has to investigate and issue a decision within a reasonable period of time (e.g. in Austria within six months). Under the GDPR, different DPAs often have to cooperate to reach a decision, for example if the affected user and the company involved are not located in the same country. If the DPA does not decide before the given deadline, or if the data subject does not agree with the legal reasoning, the decision can be appealed to the competent courts.

2.3.2 Lawsuits

There are two types of lawsuit. The first is a lawsuit aimed directly at a company. These actions usually cost more than complaints, but are often an even more powerful tool. One advantage is that lawsuits are not subject to a cross-border procedure, as would be the case with a complaint against a company based in a different Member State. For example, a cross-border procedure would apply if a complainant lives in Austria, but the targeted company is based in Ireland.

Another type of lawsuit is in the appeal process of a complaint. This type of legal action is directed against the authority's decision. The court can refer a case to the next instance, up to the Court of Justice, which then has to decide on fundamental questions of legal interpretation.

2.3.3. How do we come up with project ideas?

On the one hand, *noyb* receives tips about privacy violations from our supporting members, by the general public or whistleblowers; on the other hand, *noyb*'s legal team identifies potential projects based on the following factors:

- **High and Direct Impact:** A case or project should have a direct impact on as many people as possible, e.g. by targeting an entire industry or a common practice across different industries and Member States. In addition, we aim to scale up our projects to further increase the impact and to encourage compliance in general through the so-called spill-over effect.

- **High Chances of Success:** As a donation-funded organisation, *noyb* must allocate funds to projects that have a high chance of success. Lost cases can backfire on the overall goal of promoting privacy and data protection. Although we aim to initiate cases with a high probability of success (e.g. because the violation is obvious and the law is clear, which is true for our "enforcement actions"), there are cases that need clarification but are worth the risk ("standard-setting cases").

- **High Input/Output Ratio:** We only engage in cases or projects that have a high input/output ratio in order to maximise the use of our resources. We therefore target the biggest players and privacy issues.

- **Strategic:** Strategic litigation is based on considering all elements that may affect the case or project and making informed decisions about them. For each case, the timing, jurisdiction, costs, fact patterns, complainants, and controllers should be assessed individually . *noyb* also monitors the activities of DPAs and courts in order to take advantage of the most favourable conditions (court fees, average processing time, expertise, etc.) for our complaints.

- **Narrow and Well Defined:** Many data controllers violate almost every article of the GDPR. In our projects, we focus only on the relevant part.

Our Projects in 2023

In total, we have filed more than 40 new complaints in various jurisdictions. Among the most significant cases in 2023 were *noyb*'s first two complaints against Meta's "Pay or Okay" system. We also stepped up our action against unlawful credit scoring, filed complaints against X and the EU Commission for the use of political microtargeting on X, complaints against Fitbit for forced consent, against Ryanair's use of invasive facial recognition and against TeleSign for secretly profiling millions of mobile phone users.

Major developments are published on the front page of our website. For an overview of ongoing projects, please visit our projects page.

3.1 New projects in 2023

3.1.1 Complaints against Meta's "Pay or Okay" system

In November 2023, Meta started to charge Instagram and Facebook users a monthly fee if they want to refuse their consent to tracking for personalised advertising.

Background. In May 2018, *noyb* filed four complaints against Meta regarding "forced consent", as the company argued that the use of personal data for advertising is "necessary for the performance of a contract". We ultimately won these cases before the European Data Protection Board (EDPB) in December 2022, forcing Meta to switch to another legal basis: Instead of implementing a consent mechanism that complies with the law, Meta switched to "legitimate interest" in April 2023. In its ruling on the case Meta v Bundeskartellamt in July 2023, the European Court of Justice (CJEU), declared Meta's handling of user data for personalised advertising illegal. The Court made it clear that the company cannot use personal data beyond what is strictly necessary to provide its core products. Any data processing that goes beyond this requires freely given and fair consent by users.

In response to this judgement, and in order to secure its current business model, Meta then decided to implement a so-called "Pay or Okay" solution, giving European users the "choice" of either consenting to be

tracked for personalised advertising – or paying up to €251.88 per year to retain their fundamental right to data protection on Instagram and Facebook.

Two complaints filed. The GDPR clearly states that consent to online tracking and personalised advertising is only valid if it is *"freely given"*. This is to ensure that users only give up their fundamental right to privacy if it is their genuine free will to do so.

Scientific research suggests that consent is highly unlikely to be freely given when people are confronted with a "Pay or Okay" system. For example, the CEO of the "Pay or Okay" provider contentpass stated that 99.9 percent of visitors agree to tracking when faced with a € 1,99 fee. At the same time, objective surveys suggest that only 3 to 10 percent of users want their personal data to be used for targeted advertising. Therefore, *noyb* filed its first GDPR complaint against Meta's so-called "Pay or Okay" system.

Article 7 (3) of the GDPR gives users the right to withdraw their consent at any time. While in the current "Pay or Okay" system, one click is enough to consent to being tracked by Meta, users can only withdraw their consent by switching to a paid subscription for Facebook and Instagram. The GDPR clearly states that withdrawing your consent must be *"as easy as"* giving it. As this is clearly not the case for Facebook and Instagram, *noyb* filed an additional complaint against Meta in early January 2024.

Results. In April 2024 at the request of the Dutch, Norwegian and Hamburg Data Protection Authorities, the EDPB adopted an opinion prohibiting large online platforms such as Facebook and Instagram from using a "Pay or Okay" System. *noyb* will keep up the legal pressure against "Pay or Okay" systems in 2024, as the possible consequences go far beyond one company and could mean the end of free consent on the internet.

3.1.2 Wide-ranging action against unlawful credit scoring

Credit reference agencies, whose services are in particularly high demand in Austria and Germany, regularly collect and process the personal data of millions of people to determine their financial reliability and sell these "creditworthiness scores" to customers like online shops, mobile phone providers, and others.

Background. This data processing and acquisition usually happens in secret, so without the knowledge or consent of people. Credit reference agencies often obtain data from address brokers that was originally collected for direct marketing purposes. In addition, some credit reference agencies try to hide the fact that, under EU law, people have a right of access to data a company has about them. Instead, these companies try to nudge people into buying a paid product. In 2023, we stepped up our legal action against such unlawful practices. At the same time, we received a number of DPA decisions in ongoing cases.

Decisions in existing cases. The year started with a decision by the Austrian data protection authority (DSB) in February. It ruled that the credit reporting agency KSV1870 isn't allowed to collect data through access requests and civil registries. Prior to that, the company stored the personal data of people who exercised their rights under Article 15 GDPR in its own database. To do this, the data subject's information was checked against the Central Register of Residents. KSV1870 was ordered to delete the illegally obtained data.

Another DSB decision followed shortly afterwards. In March 2023, the authority decided that the database of the credit reference agency CRIF was illegal and that millions of data records had to be deleted. The decision followed a *noyb* complaint against CRIF and the address trader AZ Direct for illegally trading personal data that was originally collected for advertising purposes which then led to a court case (see below).

New legal action. In June 2023, we filed another complaint against CRIF in Austria. Our case against the credit agency revealed a number of legal violations, such as the provision of incorrect credit scores, unlawful data collection and the deliberate withholding of information response to an access request.

In December 2023, *noyb* then filed a lawsuit against CRIF and the address trader AZ Direct in Austria. This lawsuit relates to the aforementioned complaint and decision of the Austrian DSB. Although the authority has confirmed in two decisions that the companies' data trading is incompatible with the GDPR principle of purpose limitation, it hasn't yet taken any measures

to stop the illegal data processing. *noyb* has therefore filed a lawsuit with the Vienna Regional Court of Civil Matters on behalf of seven affected individuals. The aim is to obtain an injunction and achieve non-material damages for the data subjects.

At the beginning of January 2024, we filed a complaint and report against the creditors' association KSV1870 with the Austrian data protection authority. Although Article 15 of the GDPR stipulates that the right of access must be free of charge, KSV uses misleading website designs to urge people to purchase a high-priced "InfoPass" instead of getting a free copy of their data. Anyone wishing to apply for an Austrian visa or to extend their residence permit must be able to prove to the immigration authorities that they can support themselves without state assistance. For this purpose, the MA35 in Vienna, for example, checks whether the person has any outstanding loans, unpaid debts or even insolvency. However, the MA35 does not have this information itself. Residence applicants must therefore request the necessary data from a creditors' organisation such as KSV. This has become a lucrative business, often at the expense of unsuspecting people. The main target of this scheme appears to be foreigners. The damage to unsuspecting victims is likely to run into the millions.

3.1.3 Political microtargeting on social media

In 2023, *noyb* has filed a number of complaints against German political parties, the European Commission and against the social media platform X (formerly Twitter) for using sensitive data for political campaigns.

Background. Microtargeting is the use of online data to tailor advertising messages to individuals, based on their online behaviour and interests. The practice is widely used in online marketing to promote specific products or services, but political parties also use political microtargeting to influence the public opinion and therefore democracy. However, political opinions are particularly protected under Article 9 of the GDPR, making the use of this practice unlawful.

Legal action. In March 2023, *noyb* filed six complaints against the German parties CDU, AfD, SPD, Die Grünen, Die Linke and the Ecological Democratic Party for using microtargeting on Facebook during the 2021 federal election. The parties tried to identify potential voters and target them with personalised election promises, which is, again, unlawful under EU law.

Even the European Commission, so an EU institution that helped implement the GDPR, has used political microtargeting. The Commission targeted users on X (formerly Twitter) based on their political views and religious beliefs, in order to drum up support for its highly criticised chat control legislation. The relevant ads were only shown to people who weren't interested in keywords like *#Qatargate*, *brexit*, *Marine Le Pen*, *Alternative für Deutschland*, *Vox*, *Christian*, *Christian-phobia or Giorgia Meloni*. This is particularly worrying as the Commission has previously raised concerns about the use of personal data for microtargeting, describing the practice as "a serious threat to a fair, democratic electoral process".

The Commission's advertising campaign violated the EU GDPR. *noyb* therefore filed a complaint with the European Data Protection Supervisor (EDPS), the supervisory authority for EU institutions.

A month later, on 14 December 2023, *noyb* followed up with a complaint against X. By enabling the EU Commission's use of targeted advertising in the first place, the company had violated both the GDPR and the DSA.

Results. The complaint against X was forwarded to the Irish DPC and is still pending. The complaint against the EU Commission is still pending with the EDPS.

3.1.4 Illegal data sharing by Fitbit

Background. Fitbit is a popular health and fitness company that was acquired by Google in 2021. When creating an account with Fitbit, European users are required to *"agree to the transfer of their data to the United States and other countries with different data protection laws"*. That means their data could end up in any country in the world that doesn't have the same privacy protections as the EU. In other words: Fitbit is forcing its users to consent to share sensitive data without giving them with clear information about the possible consequences or the specific countries their data will go to.

This results in a consent that is neither free, informed or specific – meaning that the consent clearly doesn't meet the requirements of the GDPR.

According to Fitbit's privacy policy, the data shared includes not only things like a user's email address, date of birth and gender. The company may also share *"data like logs for food, weight, sleep, water, or female health tracking; an alarm; and messages on discussion boards or to your friends on the Services"*. The data collected can even be shared with third-party companies for processing. Furthermore, it is impossible for users to find out what specific data is affected.

In violation of its GDPR obligations, Fitbit also doesn't allow its users to withdraw their consent while continuing to use its products. Fitbit's privacy policy states that the only way to withdraw consent is to delete an account, which would render the fitness tracker useless.

Complaints filed. In August 2023, noyb has filed three complaints against Fitbit in Austria, the Netherlands and in Italy, asking the competent authorities to order Fitbit to share all mandatory information about its data transfers with its users and allow them to use its apps without having to consent to data transfers.

Results. All three complaints have been referred to the Irish Data Protection Commissioner and are still pending.

3.1.5 Data sharing by mobile apps violating the GDPR

Mobile apps are a hotbed of unlawful tracking. Although these apps often have millions of users, they don't bother to comply with EU privacy laws. Instead they share private data with third parties (including ad brokers) in order to monetize their users' data. According to research by Konrad Kollnig and others, only 3.5 % of all apps give users a real choice to refuse consent.

Background. The companies' apps illegally access and share the personal data of users with third parties as soon as they are opened. Users don't have the chance to consent to or prevent the sharing of their data before it starts.

According to the ePrivacy Directive, the mere access to or storage of data on the user's terminal device is only allowed if the users gives their free, informed, specific and

unambiguous consent. However, two out of the three mobile apps did not display a consent banner when the app was launched. The third app displayed a banner that theoretically gave the complainant the choice of giving or withholding their consent. In reality, the transmission of their personal data began without any interaction on their part.

This unlawful handling of user data is symptomatic of a wider problem in the mobile app environment.

Complaints filed. In September 2023, *noyb* filed three complaints in France against Fnac (the largest electronics retailer in France), the real estate app SeLoger and the fitness app MyFitnessPal. *noyb* requests the French data protection authority (CNIL) to order MyFitnessPal, Fnac and SeLoger to delete all data that has been unlawfully processed. In addition, all recipients of the complainant's data must be informed that the complainant has requested the deletion of any links, copies or replications of their personal data.

noyb is planning to file more complaints against mobile app companies in the future in order to stop the illegal sharing of user data.

Results. All three complaints are still pending with the French data protection authority.

3.1.6 Use of invasive facial recognition by Ryanair

Background. When booking through an online travel agent, rather than directly on its website or app, Ryanair requires some of its customers to go through a "verification process" involving invasive facial recognition. According to the airline, the purpose of this process is to verify a customer's contact details, even though the airline already has all the relevant information. What's more, Ryanair doesn't require biometric scanning when a customer books directly with the airline.

Facial recognition systems require people's biometric data - a category that's specially protected by law. In fact, European data protection authorities say that facial recognition can pose "unacceptably high risks" to people. Ryanair, on the other hand, even outsources this process to an external company called GetID.

Although Ryanair claims that the legal basis for its use of facial recognition is consent, it hasn't provided comprehensible information about the purpose of this intrusive process. Without clear information, a user's consent can't be informed or specific – which means it's not valid under the GDPR.

Complaint filed. *noyb* has filed a complaint against Ryanair with the Spanish data protection authority for processing people's personal data without a valid legal basis.

Results. The AEPD has forwarded the complaint to the Irish DPC at the end of September 2023. Following an update request from *noyb*, the DPC confirmed in December 2023 that it is working on the case.

3.1.7 Authentication with Cookies to exercise Data Subject Rights

Companies use tracking cookies to identify, profile and target users with personalised advertising. Conversely, this means that cookie data can also be used to identify and authenticate users who wish to exercise their rights under the GDPR.

To find out how the industry handles cookie-based authentication, *noyb* launched a new project in February 2023. To do this, several users attached the cookies that were placed by relevant websites to their access requests as a means of identification.

However, many websites and data brokers, however, did not respond adequately to the access requests. Instead, they either asked for other forms of identification or ignored the request altogether. *noyb* therefore filed several complaints against the companies (namely PubMatic and Subito) with the Italian data protection authority for failing to respond to the access requests and to respect the principle of data minimisation.

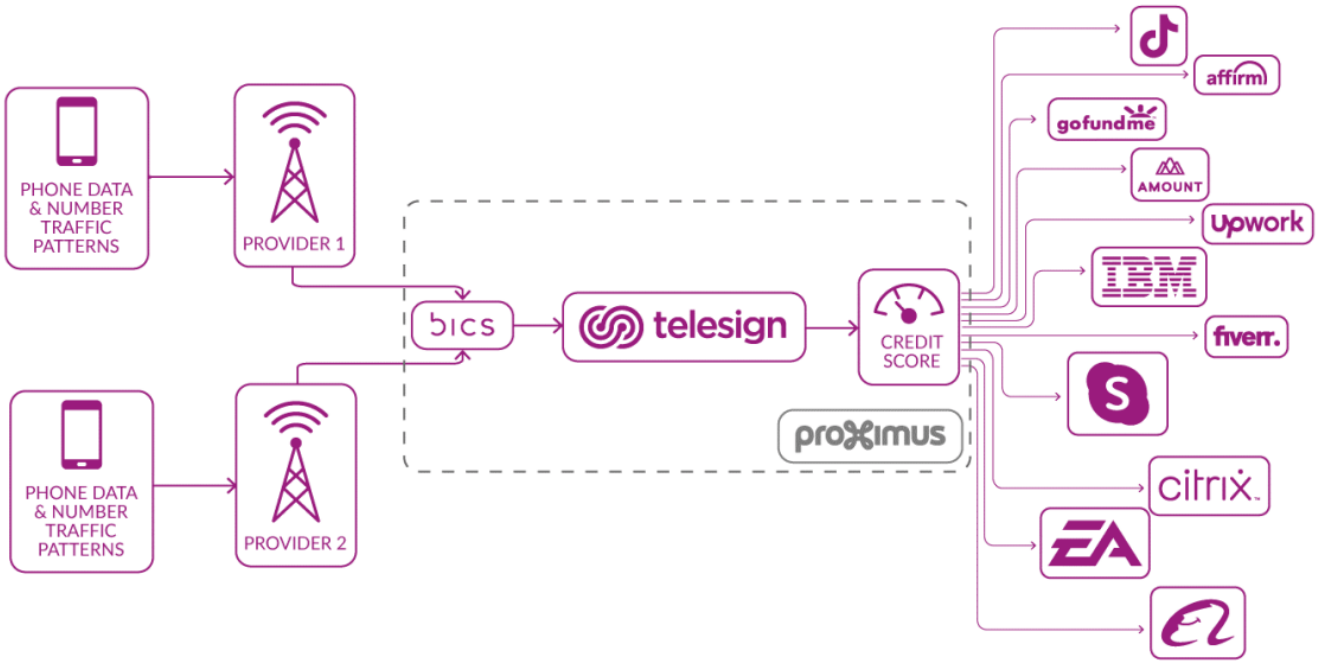
Results. The Italian DPA has confirmed that it received the complaints on the day they were filed. All three complaints are still pending.

3.1.8 TeleSign secretly profiling millions of mobile phone users

The US company TeleSign profiles millions of phone users to create a "reputation score", which is then sold to corporations such as TikTok, Microsoft and Salesforce. The data comes from BICS, a Belgian company that provides interconnection services to various mobile phone companies around the world.

Background. BICS enables phone calls, roaming and data flows between different communications networks and services in different parts of the world. By processing phone customer data, BICS obtains detailed information (e.g. the regularity of completed calls, call duration, long term inactivity, range activity, or successful incoming traffic) on half of the world's mobile phone users.

Based on this data, TeleSign creates a "trust score" between 0 and 300 points. This score is sold to companies (e.g. TikTok, Salesforce and Microsoft) who then decide whether to allow users to sign up to a platform or whether to require an SMS verification first. TeleSign verifies over five billion unique phone numbers per month, representing half of the world's mobile phone users.



As part of *noyb*'s complaint, several mobile users used their GDPR rights to obtain copies of their data from TeleSign, BICS and their national mobile provider. None of the mobile operators listed TeleSign as a recipient or were aware that user data was being sent to TeleSign. At the same time, TeleSign confirmed that it had the phone number and provided the "trust score" assigned to their number, such as "medium-low"

Complaint filed. As a result, *noyb* has filed a complaint against TeleSign with the Belgian data protection authority in June 2023. While there are some situations where personal data can be used for security purposes without consent, the secret use of telecommunications data on the majority of the world's mobile phone users is not in line with EU and national data protection law. In addition to an order to stop the transfer of data to TeleSign, the Belgian DPA can issue a fine up to € 236 million, or 4 % of the global turnover of the Proximus Group, which owns BICS and TeleSign.

Results. The complaint is still pending with the Belgian data protection authority.

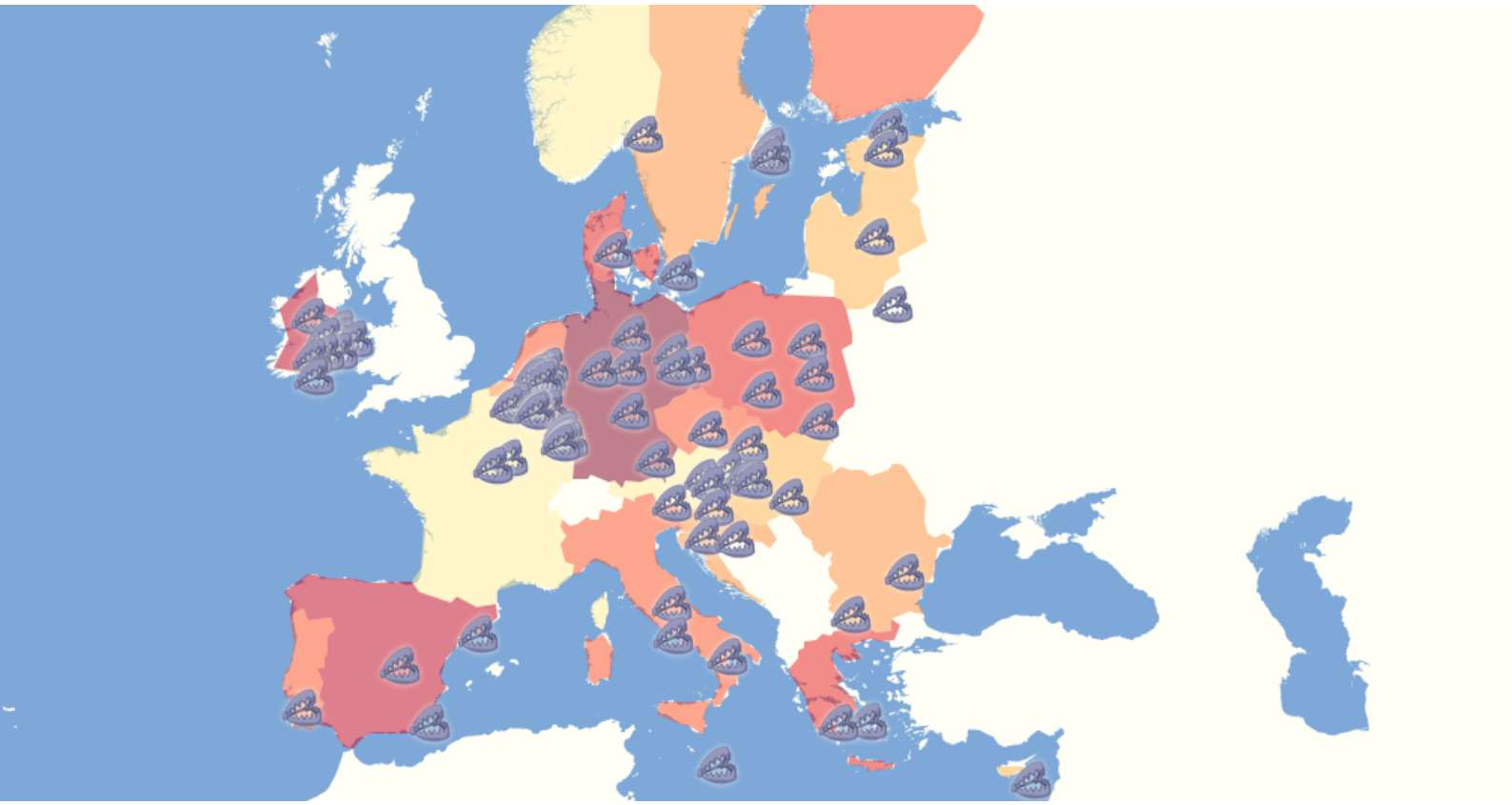
3.1.9 15 complaints against Belgian news sites over unlawful cookie banners

On 19 July 2023, noyb has lodged complaints against 15 Belgian news sites using deceptive cookie banners with the Belgian DPA. Among them are large TV channels like RTL Belgium, the public service broadcaster VRT, but also newspapers like Het Laatste Nieuws and L'Avenir.

Background. Although their websites already were subject of a DPA investigation in the past years, they were never ordered to change their unlawful cookie banners. The reason: The procedure was closed with a questionable settlement. According to the terms of said settlement, the publishers agreed to paying € 10.000 – but weren't ordered to comply with any of the obligations under the GDPR. In its decision, the Belgian DPA didn't even bother to explain why the cases were settled and not followed by an order to comply.

In its complaints, *noyb* requested the Belgian DPA to investigate the cases once again and order the 15 news sites to change their unlawful cookie banners. In case of non-compliance, the DPA can issue a fine of up to 4 percent of the annual turnover of the companies behind the websites.

Results. In the meantime, some of the complaints have been settled whereas the rest are still pending with the Belgian data protection authority.



3.2 GDPR Procedures Regulation

In an effort to improve cross-border investigations, the GDPR states that data protection authorities must cooperate with each other – but fails to provide details on how this cooperation should work in practice. This has led to a serious lack of cooperation and several conflicts between DPAs. Some member states have even adopted procedural rules aimed at undermining GDPR procedures. See GDPR trap map above

At the beginning of July 2023, the EU Commission therefore introduced a proposal for a GDPR Procedures Regulation, which, in theory aims to improve the enforcement efforts of DPAs in cross-border cases. In reality, the proposal seems to be based mainly on the demands of some DPAs' to remove citizens from procedures with the alleged aim of simplifying them.

While some key elements that would lead to faster procedures – such as substantial deadlines for the lead supervisory authority – are largely missing, the Commission's approach would have tipped the already problematic balance of arms in data protection cases even further in favour of companies. While citizens would have only minimal rights to be heard, the draft provides for extensive rights for the companies: They would be heard throughout the procedure and have access to the case files. This could entrench existing problems before opaque regulators such as the DPC rather than solving them.

noyb has reacted quickly to the proposed regulation and published a comprehensive list of measures that, in *noyb*'s opinion, could actually lead to an improved cross-border cooperation and faster, more effective enforcement actions. The proposal is currently with the European Parliament and Member States, who must agree on a final version. *noyb* will continue to monitor the process closely and advocate for the strengthening of citizens' rights.

3.3 Knowledge Sharing

As well as working on complaints and court cases, *noyb* is also actively disseminating GDPR developments to professionals and the public, in particular through our public wiki GDPRhub and the newsletter GDPRtoday.

3.3.1 GDPRhub and GDPRtoday

In October 2019, *noyb* launched a newsletter project aimed at summarising, translating and publishing decisions of data protection authorities and court rulings from all European Member States. For this purpose, *noyb* created a database with all the national sources across Europe for DPA and court decisions and employed a tool to both monitor them and to create notifications for any updates. Subsequently, in February 2020, GDPRhub and GDPRtoday were launched: a free and open wiki where anyone can find and share GDPR insights from across Europe, paired with a newsletter where we collect recent decisions and a commentary on the latest developments in the world of privacy and data protection.

The content on GDPRhub is divided into two separate databases: decisions and knowledge. In the decisions section, we collect summaries of decisions by national DPAs and European and member state courts in English. The knowledge section contains commentaries on GDPR articles and DPA profiles. Over the course of 2023, the number of decisions collected and summarised has grown to more than 3,000, with more than 10,000 subscribers to the weekly GDPRtoday newsletter. More than 300 active volunteers help *noyb* to collect and summarise these decisions in jurisdictions *noyb* could never cover in-house due to language barriers.

3.4 Updates on ongoing projects

So far, *noyb* has filed 836 individual complaints with various data protection authorities across Europe. Only 283 of these cases have been decided by the competent authorities, most of which were either closed or concluded with a settlement because the company had remedied the breach. Some cases were only partially decided, and several cases are currently before the national courts because the authorities did not decide within the legal deadline or because *noyb* appealed the decision. An overview of all ongoing cases can be found here.

3.4.1 Two fines against Meta amounting to more than € 1.5 billion

2023 was a year of big fines for Meta. Following a binding decision by the EDPB, the Irish DPC ordered the social media corporation to pay a whopping € 390 million in early January 2024. At the same time, Meta was banned from using personal data for advertising without asking its users for their explicit yes/no consent in line with Article 6(1)(a) GDPR. Before that, Meta had attempted to circumvent this requirement by claiming a so-called "contractual necessity" under Article 6(1)(b).

The decision followed two complaints filed by *noyb* on behalf of one Austrian and one Belgian user on 25 May 2018, meaning that it took the competent authority four and a half years to reach a decision after the EDPB had overturned its first draft decision in December 2022.

At the end of May 2023, Meta was fined € 1.2 billion and ordered to stop transferring Europeans' personal data to the United States. The company is subject to US surveillance laws such as FISA 702, which allows the US government to spy on non-US citizens without probable cause or judicial approval.

This contradicts EU law, which requires "essentially equivalent" protection for data transferred outside the European Union. US companies like Meta can't meet this requirement. This also was confirmed by the CJEU's decision to annul both the "Safe Harbor" and "Privacy Shield" agreements in its Schrems I and Schrems II rulings in 2015 and 2020 respectively. Meta has ignored these judgements for the last years, which ultimately led to the € 1.2 billion fine and an order to return all personal data to its EU data centres.

3.4.2 First major fine for the usage of Google Analytics

Following *noyb*'s 101 complaints on unlawful EU-US data transfers from 2020, the Swedish data protection authority (IMY) issued the first major fine for using Google Analytics in July 2023. Although many other European authorities (e.g. Austria, France and Italy) have already found the use of Google Analytics to violate the GDPR, this is the first fine imposed on companies for using Google Analytics, despite the CJEU's rulings on EU-US data transfers. Telecommunications provider Tele2 was ordered to pay the equivalent of € 1 million (12 mio SEK), while the online retailer CDON had to pay SEK 300,000. The IMY also points out that the so-called "supplementary measures" for data transfers were not sufficient.

3.4.3 Spotify fined € 5 million for GDPR violation

Following a *noyb* complaint and litigation over inaction, the Swedish Data Protection Authority (IMY) has issued a fine of 58 million Swedish Crown (about € 5 Million) against Spotify in June 2023. The music streaming service didn't fully comply with the GDPR's obligation to give users access to all their data, and information about how their data is being used. The complaint was already filed in 2019, and was not decided for more than four years.

3.4.4 Advertising company CRITEO fined € 40 million

At the end of June 2023, the French data protection authority (CNIL) fined CRITEO, a major European online advertising and tracking company, €40 million for its violation of data subject rights and its failure to prove that it obtained valid consent.

The decision followed a complaint filed by *noyb* and Privacy International in December 2018, which targeted the lack of an adequate option to withdraw consent. The complaint triggered an extensive investigation by the CNIL, which widened the scope to other areas and found additional GDPR violations: among others, lack of transparency, failure to comply with the right to erasure and the right of access.

3.4.5 Majority of the database of Austrian credit agency CRIF is illegal

At the end of March 2023, the Austrian data protection authority decided that the credit reference agency CRIF had illegally processed the data of millions of people.

CRIF has collected the addresses, dates of birth and names of almost all Austrians in order to calculate "creditworthiness values" without ever asking for consent or having any other legal basis.

The data was originally collected for marketing purposes by the address trader AZ Direct, which means that it can only be passed on for this exact purpose. This means that it is illegal for CRIF to use it for credit reference purposes.

The data protection authority now has agreed with this assessment, meaning that millions of data records will have to be deleted.

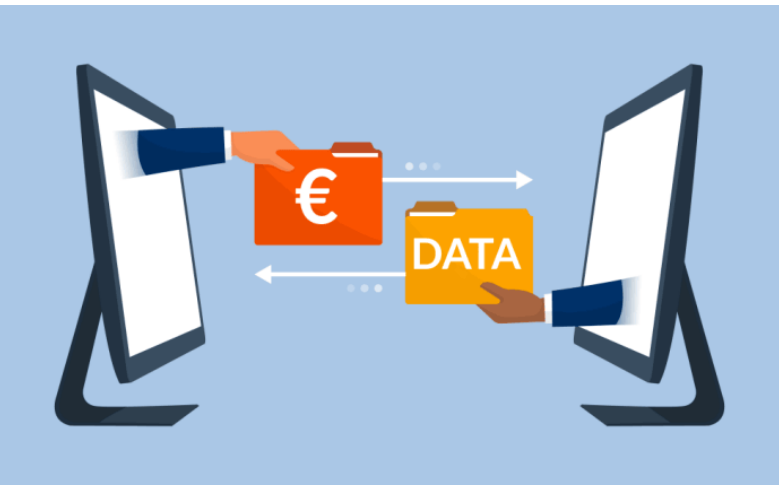
3.4.6 Right of access must include context

In 2023, *noyb* was fortunate enough to celebrate another victory at the European Court of Justice (CJEU). Following a legal dispute over a request for access to the credit reference agency CRIF, the Court ruled that users must be given not only a copy of their raw data, but also information about the context of the data in an understandable way. This can also include the documents containing personal data. The term "copy" means a true and accurate reproduction of the actual data.

CRIF initially replied to the data subject with only a list of the data processed about him. The data subject, who requested a copy of all data relating to him, including database extracts, lodged a complaint with the Austrian data protection authority.

The case eventually ended up before the Austrian Federal Administrative Court, which referred several questions to the CJEU for a preliminary ruling on the scope of the right to obtain a "copy of data" under Article 15(3) GDPR.

In its ruling, the CJEU emphasises that the purpose of the GDPR is to strengthen and precisely define the rights of data subjects. The right of access is particularly important in this context, as it enables data subjects to exercise other rights, such as deletion, rectification or objection - which would only be possible to a limited extent without knowledge of the specific data processed.



The CJEU also emphasises the need to contextualise the information provided. It is not enough to for companies to simply provide list of raw data. The data must be made available to the data subject in full, in context and true to the original form. This is particularly important in the case of data that is generated from other data - as in the present case, where credit scores were calculated based on the basis of the data held on of the data subject. Here, as the CJEU emphasises, it will regularly be necessary to provide excerpts of documents, entire documents or even database extracts. Otherwise, it is difficult for the data subject to understand the true meaning of the data, but also if the data is manipulated, inconsistent or only partially provided.

3.4.7 "Pay or Okay" on derStandard.at and heise.de declared illegal

noyb has also made some progress regarding "Pay or Okay" systems. So-called "Pay or Consent" systems give users the choice between paying for a monthly subscription or having their personal data processed for advertising and many other purposes.

In April 2023, the Austrian data protection authority decided that the so-called "PUR" subscription offered by the Austrian daily newspaper derStandard was illegal in its current form.

While the DPA confirmed the general permissibility of "Pay or Okay", it specified that users must be given the opportunity to say "yes" or "no" to each specific data processing, as required by the GDPR. It is still unclear how a "subscription obligation" is supposed to work in case a person says "no".

As the DPA's decision leaves a number of questions unanswered, *noyb* filed an appeal with the Austrian Administrative Court in May 2023. The appeal is still pending.

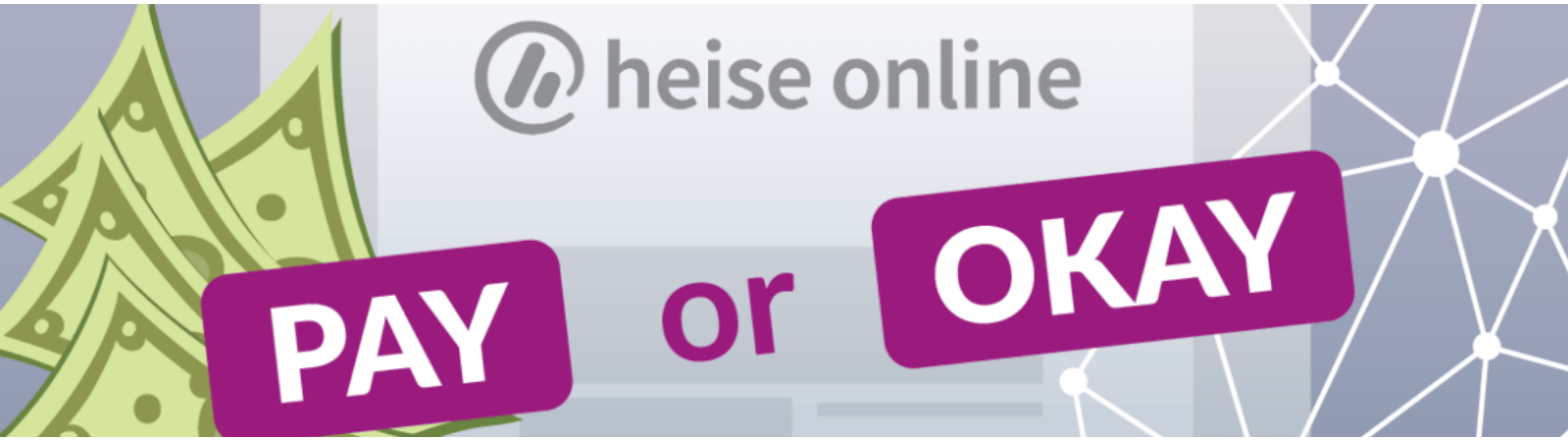
In June 2023, the data protection authority of Lower Saxony (LfD) followed suit. It decided that the

Pay or Okay approach taken by the tech news site heise.de in 2021 was unlawful.

Although it considered that "Pay or Okay" could be permissible in principle, it found that the approach taken by the news site was not in line with the law because it didn't offer the option of giving explicit consent for certain purposes – a decision, that is in line with the guidelines of the Conference of German Data Protection Authorities (DSK).

In March 2023, the DSK explicitly expressed its concern about the lack of specific and transparent consent on websites using "Pay or Okay" models, while not questioning the broader issue of users having to pay exorbitant prices to keep their personal data private.

In addition to the issues around "Pay or Okay", the LfD found that heise.de used unlawful and methodical nudging to influence users for its own benefit. The LfD also found that the user's consent was not informed, specific or freely given. Furthermore, it wasn't easy enough to revoke a previously given consent at a later point in time – leading the LfD to conclude, that there was no legal basis for processing the user's data.



3.4.8 European Data Protection Board supports noyb's call for fair yes/no cookie banners

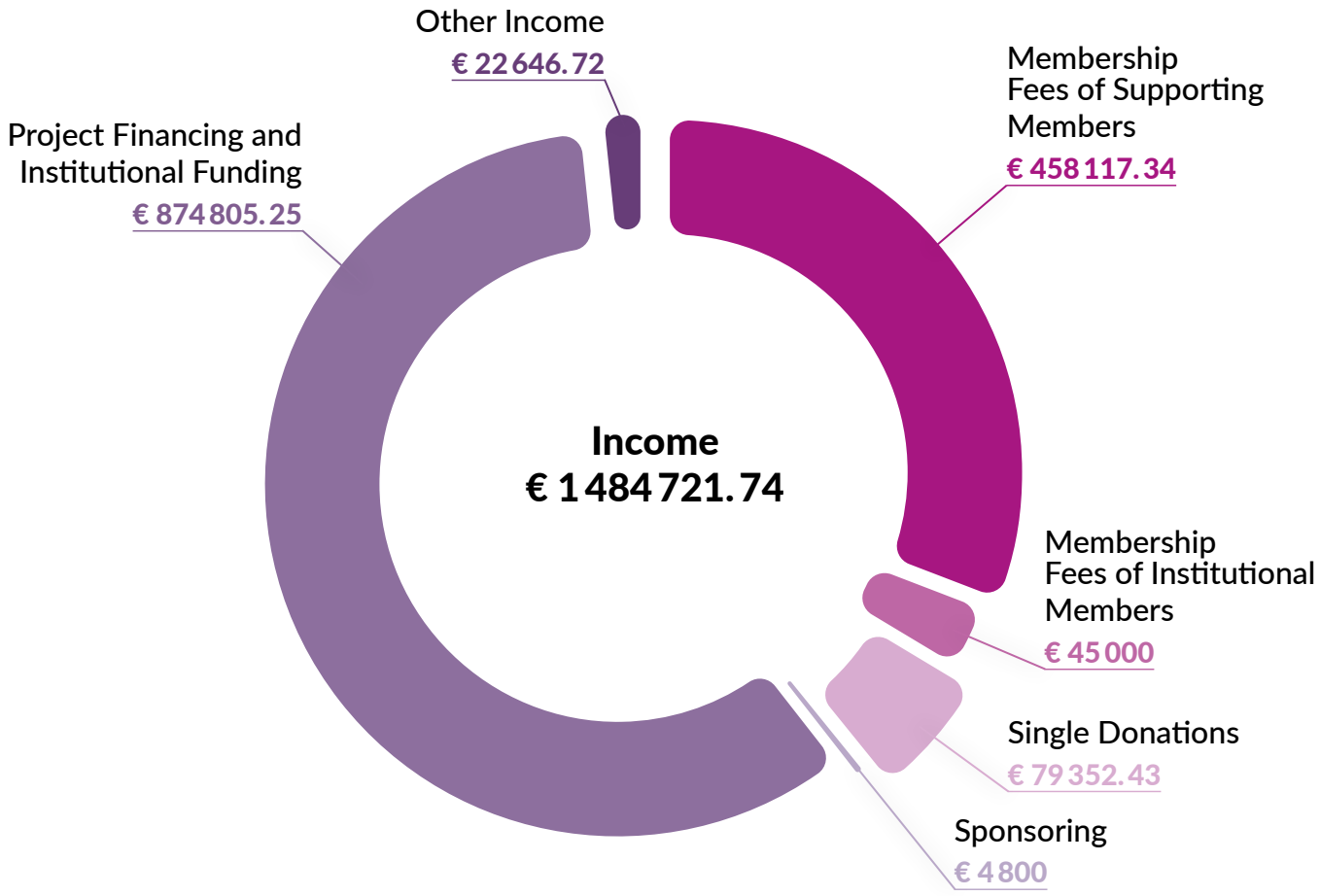
Following more than 700 *noyb* complaints against unlawful cookie banners, a task force within the European Data Protection Board (EDPB) published a report on the subject in January 2023.

The EDPB report largely supported the *noyb* complaints, stating that the following practices are clearly unlawful under EU law:

- No reject option on the first layer (but hidden in a sub-layer)
- Pre-ticked boxes instead of active consent
- Tiny links in another text to refuse consent
- Links outside the cookie banner to refuse consent
- Claiming legitimate interest for installing non-essential cookies (and not asking for consent)
- Not offering a permanent option to withdraw consent

The draft decision is the result of the DPAs' cooperation within the EDPB's task force on cookie banners, which was launched in September 2021 following the filing of more than 500 cookie banner complaints by *noyb*. The draft report reflects the lowest common denominator in the DPAs' interpretation of the applicable law, setting a minimum threshold for assessing consent cookie banners. Many national guidelines even go further, and *noyb* is equally of the view that the law requires further protection, for example under the GDPR's 'fairness' requirement.

Our Finances



Membership Fees of Supporting Members
fees from 5 200 supporting members

Membership Fees of Institutional Members
City of Vienna (€ 25 000), Austrian Chamber of Labor (€ 20 000)

Single Donations
individual donations ranging from € 1 to € 18 000

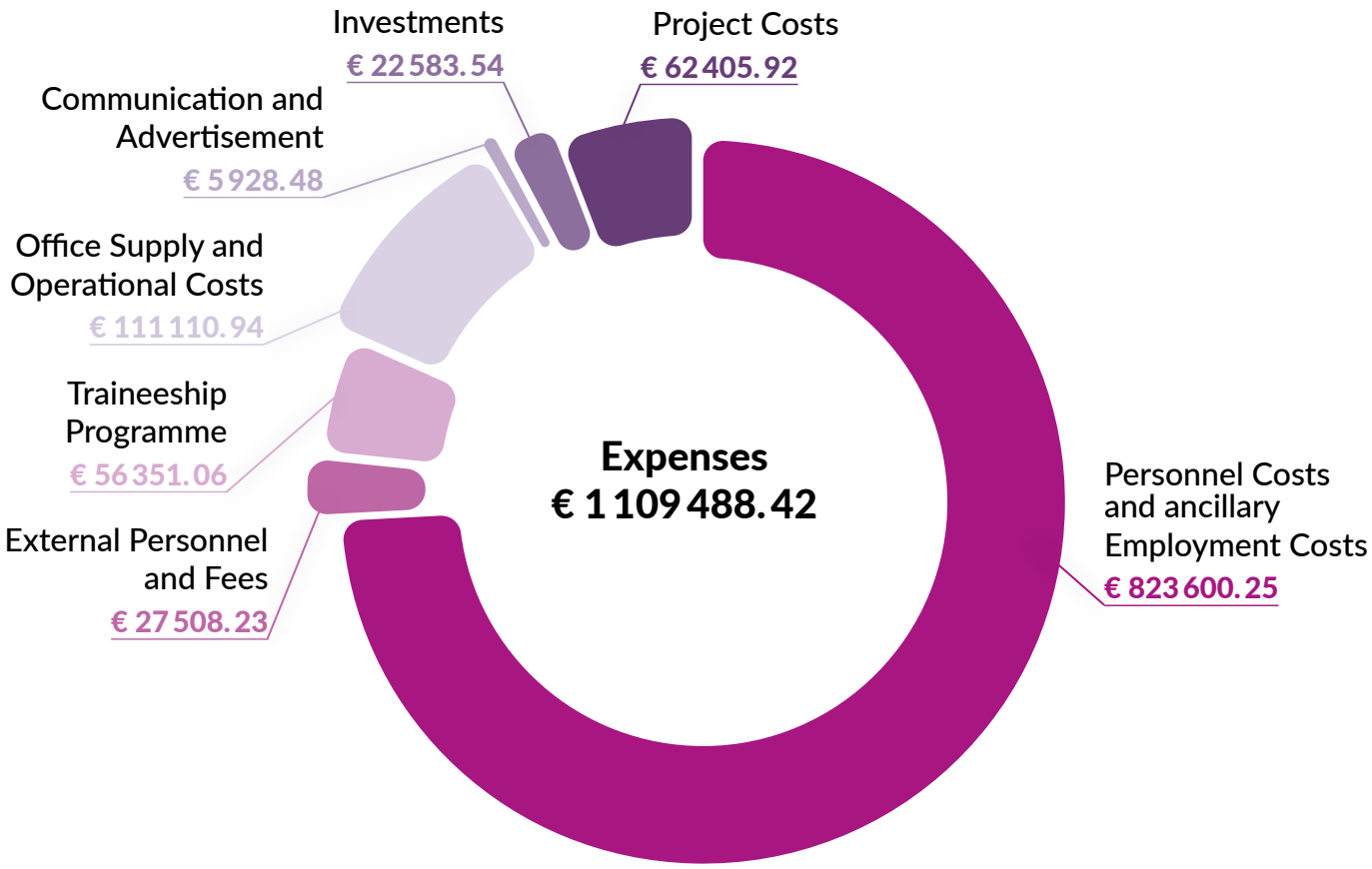
Sponsoring
Jonas Breyer (€ 1 000), Freedom Internet BV (€ 1 000), foundata (€ 1 000), LamaPoll (€ 1 000), GDPRtoday Sponsoring (€ 800) Dialog-Mail (€ 21 000 in kind)

Project Financing and Funding
Austrian Ministry for Social Affairs (€ 42 000, core funding), Sub3 (€ 100 000 core funding), Open Society Foundation grant for 2023-2026 (€ 323 894. 13), BEUC (€ 25 050), Forbrukerradet (€ 5 000), DFF (€ 28 687. 58), Luminate (€ 350 173. 54)

Other Income
professional fees (€ 1 415. 81), participation in Stichting CUIC (€ 12 500), remuneration for COVID isolation of employees according to§32 EpiG (€ 7 854. 86), interest

noyb is using the cash flow method of accounting therefore expenses and income are accounted for the year the occur.

Our Finances



- **Personnel Costs and ancillary Employment Costs**
- **Extra Personnel and Fees**
  e.g. external staff / freelancer / services (non-legal)
- **Traineeship Programme**
  daily allowances, housing, transportation tickets for extraordinary members (trainees)
- **Office Supply and Operational Costs**
  rent, electricity, cleaning, office supplies, insurance,...
- **Communication and Advertisement**
- **Investments**
  furniture, hardware, software and alike
- **Project Costs**
  fees for external lawyers, court fees, and alike

noyb is using the cash flow method of accounting therefore expenses and income are accounted for the year the occur.

noyb in the Media

Nach Böhmermann-Recherche

Datenschützer gehen gegen Parteienwerbung auf Facebook vor

DER SPIEGEL

Targetleaks >>

NEWS

EU hits Meta with record €1.2B privacy fine

Tech giant transferred Europeans' data to the US unlawfully, I regulator said.

LISTEN

POLITICO

Meta Record Fine >>

TECH

Meta Fined Over $400 Million in EU for Serving Ads Based on Online A

THE WALL STREET JOURNAL.

Meta Fine >>

Sam Schechner Follow

Denuncian a Ryanair por forzar a los asajeros que no compran el vuelo en su eb a someterse a reconocimiento facial

elDiario.es

Periodismo a pesar de todo

Ryanair >>

Technology

Meta Platforms' paid ad-free service targeted in Austrian privacy complaint

By Foo Yun Chee

November 28, 2023 10:51 AM GMT+1 · Updated 8 months ago

REUTERS

Pay or Okay >>

[1/2] A blue verification badge and the logos of Facebook and Instagram are seen in this picture illustra January 19, 2023. REUTERS/Dado Ruvic/Illustration/File Photo Purchase Licensing Rights

PIXELS · DÉSINFORMATION

Le Monde

European Commission >>

Le Monde avec AFP et Reuters

Publié le 17 novembre 2023 à 16h41, modifié le 17 novembre 2023 à 18h05 · Lecture 1 min.

Ajouter à vos sélections

Bruxelles redouble de précautions face à la désinformation qui sévit sur le réseau social X. La Commission européenne a demandé à ses services de suspendre leurs campagnes publicitaires sur la plate-forme, a fait savoir le porte-parole Johannes Bahrke, vendredi 17 novembre.

Les plus

noyb in Numbers

5245
Supporting Members
from 53 different countries

17
Team Members
from 7 different countries

12
Trainees
from 10 different countries

40 **Complaints** filed in 2023

553 **Complaints** currently pending

109 **Cases** closed, withdrawn or lost by authorities

>1.55 billion € in fines

45
Press Releases

12
Newsletters & Member Updates

>64 000
Followers on six social media platforms

GDPR hub

3088 **Summaries**

312 **Active Country Reporters**

10 075 **Subscribers to GDPRtoday**

12 **Country Reporter Meetings**

Thank you to our sponsors and partners for supporting our work and making privacy a reality!

Stadt Wien

Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

dialog Mail
eMarketing Systems

freedom internet

LamaPoll

foundata

JONAS BREYER
LAW FIRM | WWW.KANZLEI-BREYER.DE

noyb **European Center for Digital Rights**

Imprint:
noyb – European Center for Digital Rights

Goldschlagstraße 172/4/3/2
1140 Vienna – Austria

ZVR: 1354838270