European Center
for Digital Rights

Annual Report

2024

noyb.eu

Contents

Preface

Almost 7 years after the GDPR came into force, *noyb* remains to be one of the leading European forces pushing for the fundamental right to data protection for all users. Immediately after the GDPR came into force on **25 May 2018**, *noyb* filed its first cases against major companies such as Google and Meta – and has maintained the pressure ever since. To date, our legal work has resulted in administrative fines totalling **€1.69 billion.**

Nevertheless, we unfortunately see that the lack of enforcement by data protection authorities (DPAs) and limited interest by courts makes *noyb's* work more relevant – but also more challenging every year. We also witness increasing pressure on DPAs to interpret the GDPR in an (even more) business friendly way. There is an increasing amount of open interference with (theoretically) independent authorities. This fundamentally undermines the GDPR's enforcement structure. In theory, courts should exercise oversight of DPAs. In reality, however, many courts are happy if they don't have to deal with novel digital matters and the GDPR, and employ increasingly aggressive arguments to reject cases.

While we continued to work on our almost **400 pending cases**, we have also filed **36 new complaints** against major companies across Europe in 2024. This has allowed us to tackle issues such as credit scoring, online tracking, the use of facial recognition systems, data subject rights – and unlawful data use to train artificial intelligence. Together with the hype around AI tools such as ChatGPT, concerns over potential data protection and privacy issues have intensified. Since the technology and industry are developing rapidly, we were required to react quickly to combat GDPR violations. Judging from the approach by AI companies (to just take the data and ask later), we expect that AI issues will take up significant resources in the coming years.

Among the most significant cases of 2024 are *noyb's* first complaints against Meta's and Twitter's (X) plan to unlawfully take the personal data of European users to train their AI systems. We filed **11 complaints against Meta** in June 2024, resulting in a pause of the training plans for the rest of the year. In August, we followed up with **9 complaints** against Twitter's very similar AI plans.

On 4 October 2024, *noyb* **won another case** against Meta before the European Court of Justice The ruling in case C-446/21 massively limits Meta's use of personal data for online advertising. It also limits the use of publicly available personal data to the originally intended purposes for publication.

We also continued to invest time and effort in expanding our data protection knowledge database GDPRhub. By the end of 2024, it already contained more than **4,100 decisions and judgements** from across Europe. This project is made possible by our more than **230 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 2025, 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 strengthened our public relation and media initiatives to

highlight privacy violations. 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 **35 press releases,** published hundreds of social media posts on seven different platforms and continue to be an active voice in the public discourse on privacy and data protection.

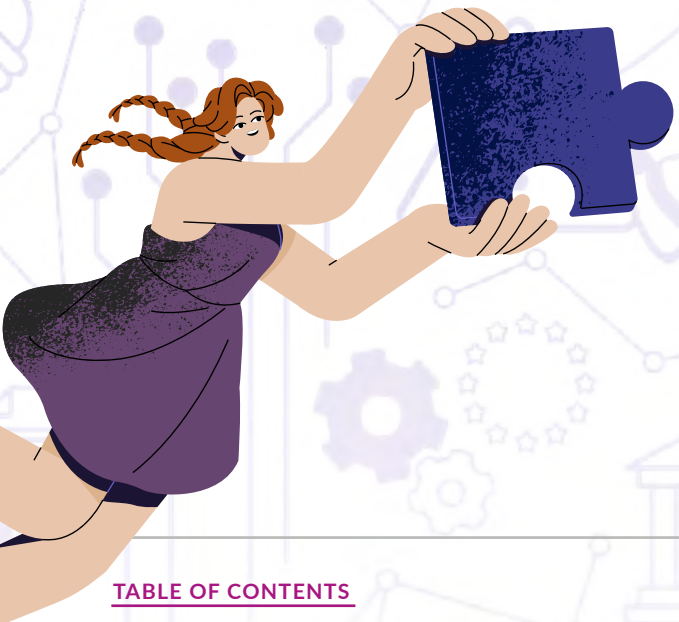
None of our work would have been possible without our **5,250 Supporting Members, institutional members and every individual person** who has donated to *noyb*. We deeply appreciate this support, especially in times of multiple crises. Your generosity and commitment enable us to continue our work and 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. Since 2024, *noyb* is now an approved **Qualified Entity** in Austria and Ireland, which enables us to bring injunctions and redress measures such as class action lawsuits. 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 were also closely following the ongoing negotiations on a GDPR Procedural Regulation. Theoretically, the file is supposed to improve cross-border cooperation between data protection authorities and to simplify procedures. In reality, the final text could have the opposite effect and actually restrict the rights of the people concerned – or at least make enforcement much slower and more complicated.

With many challenges ahead, but also with many new angles to move things forward, 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 six years!



Max Schrems
HONORARY CHAIRMAN

About *noyb*

2.1 Our Mission

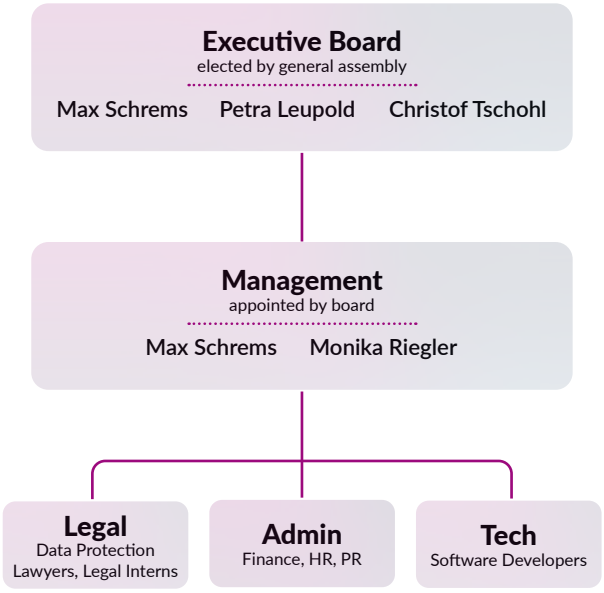
noyb follows the idea of **targeted and strategic litigation** in order to strengthen the right to privacy: In practice, we pursue this goal by thoroughly analysing and prioritising privacy violations, identifying the legal weak spots of these cases and litigating them using the best possible strategy 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.

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.

Read more about *noyb* here.

2.2 Who we are

2.2.1 Organigram and Governance



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. Max Schrems has been the pro-bono Managing Director at *noyb* since the beginning. As Operations Director, Monika Riegler is responsible for all administrative matters as well as the PR and IT department of *noyb*.

2.2.1.1. Executive Board

Max Schrems
MAX SCHREMS - HONORARY CHAIRMAN AND 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 and Privacy Shield) 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.

Petra Leupold
HONORARY BOARD MEMBER

Petra Leupold is the Head of Litigation of the Austrian Consumer Protection Association VKI. She brings invaluable experience in general consumer protection and litigation.

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.

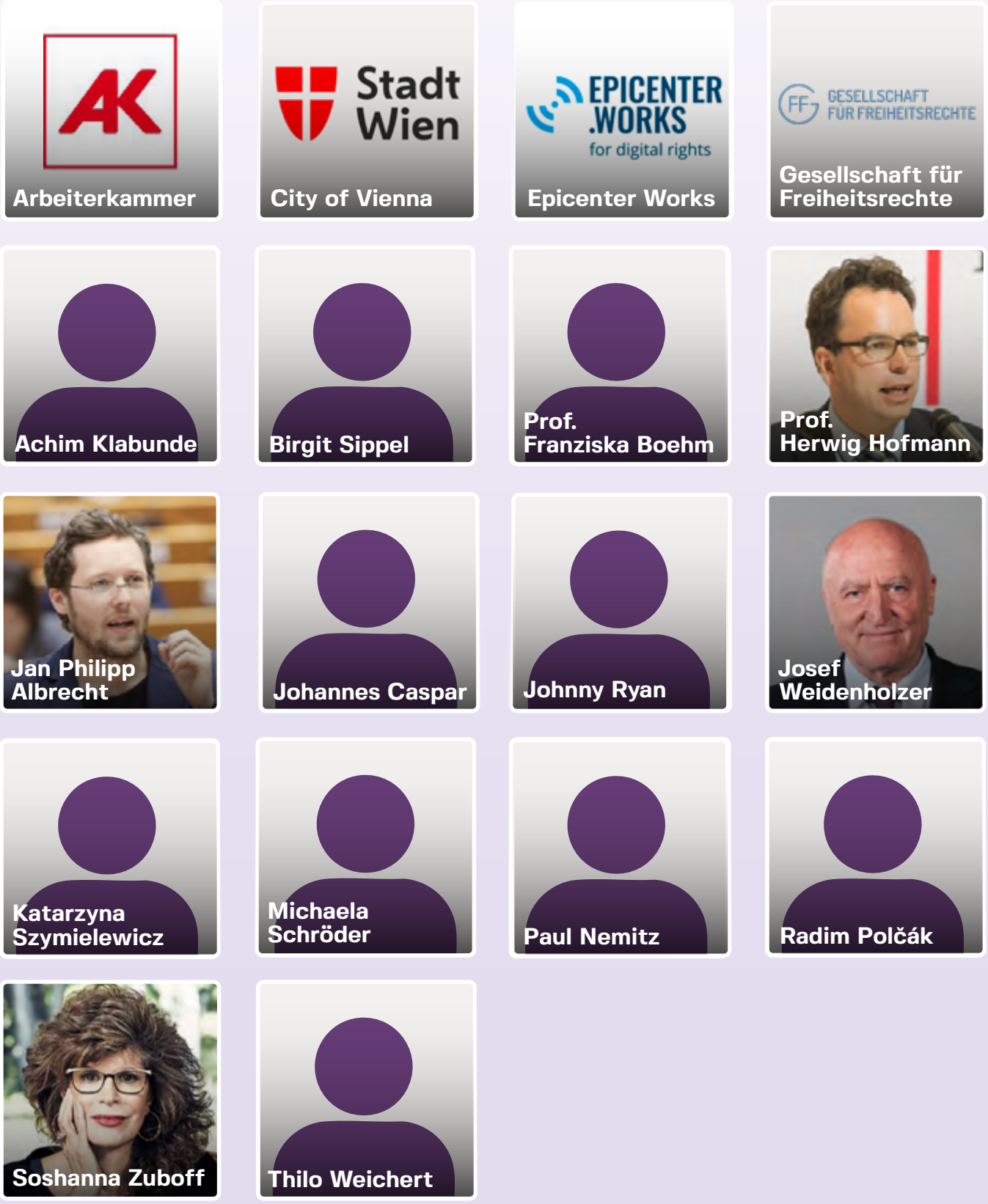
Christof Tschohl
HONORARY BOARD MEMBER

Christof Tschohl successfully overturned the Austrian data retention law and was the founder and chairman of the NGO epicenter.works, which is dedicated to defending our rights and freedom on the Internet. Furthermore, he is Research 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.

2.2.1.2. General Assembly

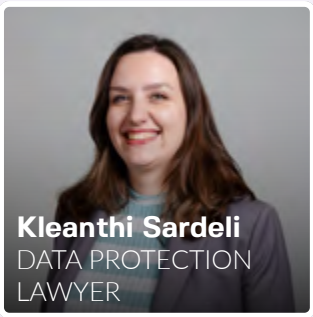
noyb's general assembly consists of four institutional members and - including our Executive Board - 17 individuals with a strong academic or legal background in the field of data protection and the GDPR in particular.

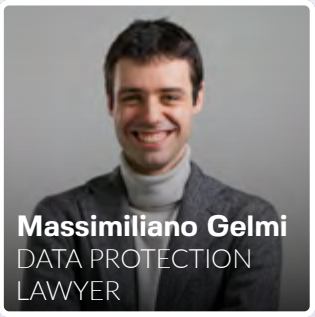


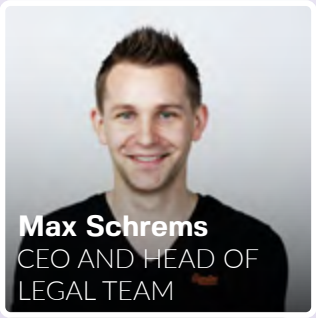
*as of Dec 2024

2.2.1.2. Staff – Legal Team

For our office we are building a pan-European team of lawyers and experts. Besides answering initial inquiries and helping our members, the core task of the office is to work on our enforcement projects and to engage in the necessary research for strategic litigation. Our office team is the key factor of making sure that privacy becomes a reality for everyone.





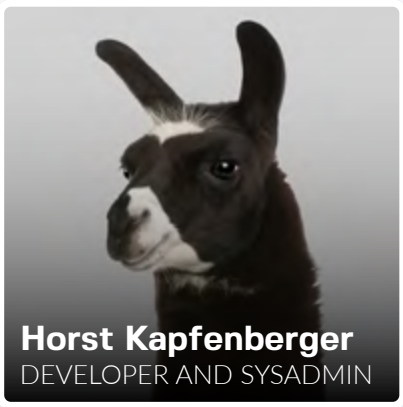


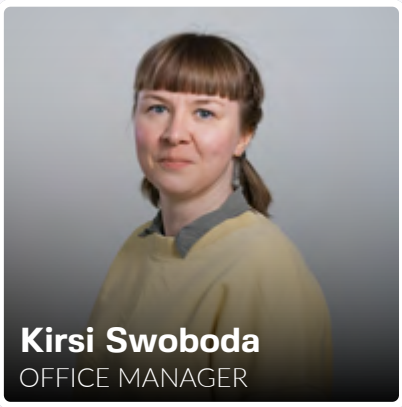
2.2.1.3. Legal Traineeships

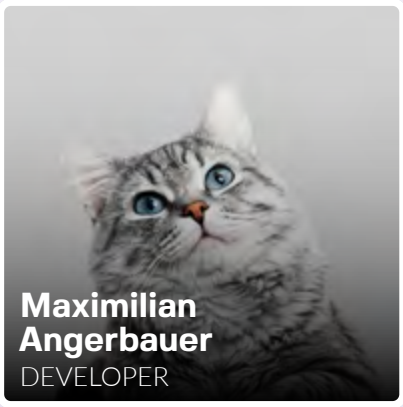
Since October 2018, *noyb* has been offering **legal traineeships** for university graduates with a strong interest in privacy law. Our trainees gain experience in legal research, factual investigation, and drafting privacy complaints. They also work on *noyb's* publicly available database, GDPRhub, and *noyb's* weekly newsletter, GDPRtoday. In 2024, **13 trainees** from **nine different countries** joined *noyb* for a period of three to six months.

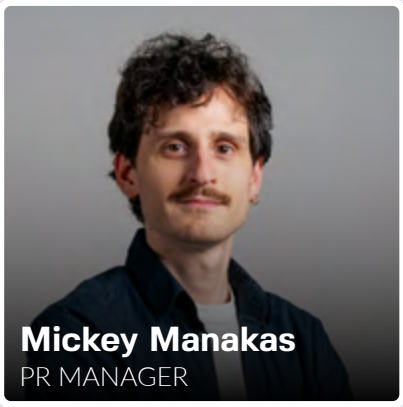
**as of Dec 2024*

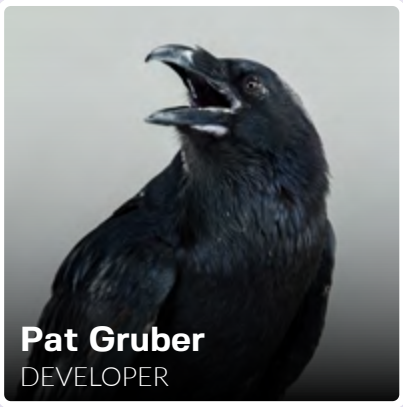
2.2.1.4. Staff — Office & Tech Team

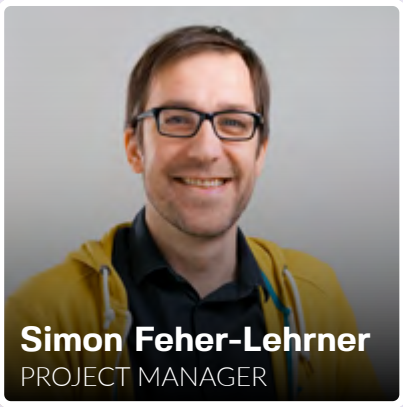


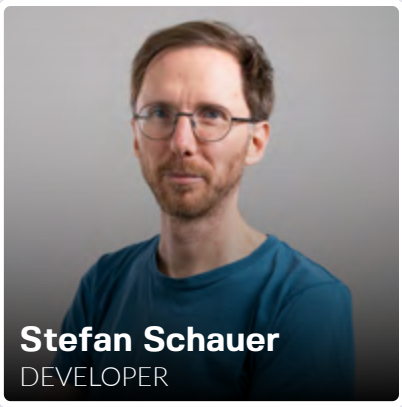












*as of Dec 2024

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 identifying privacy violations, focusing on 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, enforcement actions** and going forward, also **collective redress.**

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.

Collective Redress Actions: *noyb* has been approved as a so-called Qualified Entity under the EU Collective Redress Directive in both Austria and Ireland. This enables us to bring injunctions and redress measures like a class action in any EU Member State. In Europe, only non-profit organisations are allowed to bring such actions.

Injunctions generally prohibit a company from engaging in illegal practices, including any GDPR violations. Redress measures allow a European version of a class action lawsuit, where thousands or millions of users could be represented by *noyb* and – for example – ask for non-material damages in case of unlawfully processed personal data.

noyb has in the past years prepared the organisational and technical means to bring collective redress actions and expects to start the first cases in 2025.

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").

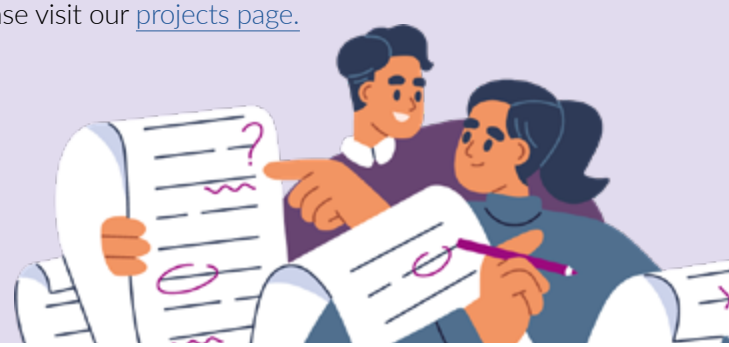
- **High Input/Output Ratio:** We only engage in cases or projects that have a high input/output ratio in order to maximise the use of our resources. We therefore target the biggest players and privacy issues.

- **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.

Our projects in 2024

In total, we have filed **36 new complaints** in various jurisdictions. Among the most significant cases in 2024 were *noyb*'s first complaints against unlawful data processing in artificial intelligence systems. We filed **11 complaints against Meta** and **9 complaints against Twitter (X)** to stop their plans to feed all the data of their users into an undefined AI system. On top of that, we tackled unlawful online tracking by major internet browsers such as **Firefox** and **Google Chrome** and filed a complaint against **Microsoft's** tracking of school children. We haven't let up in our efforts to take action against unlawful credit scores either: We filed complaints against **SCHUFA** and **KSV1870**. Last but not least, we took on Swedish data brokers and filed two complaints against the **EU Parliament** because of a massive data breach.

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



3.1 Enforcment Actions

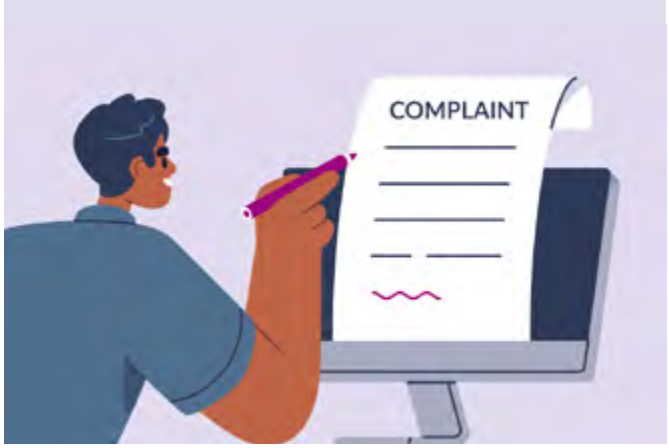
3.1.1 Artificial Intelligence

With the rapid rise of artificial intelligence and large language models (LLMs), concerns over data protection and privacy have intensified. These technologies rely on vast data sets, which can include personal information. This raises serious questions about how user data is collected, stored, and used. As the potential for misuse grows, so does the urgency for stronger safeguards. In response, *noyb* is stepping up its efforts to ensure that individuals' data rights are respected and enforced, holding companies accountable for violations and pushing for greater transparency and compliance in the age of AI.

3.1.1.1. Complaints against Meta's AI plans

Background. In May 2024, Meta had informed millions of Europeans that its privacy policy is changing once again. With these changes, Meta wanted to take all public and non-public user data it had collected since 2007 and use it for an undefined type of current and future "artificial intelligence technology". This also includes the many dormant Facebook accounts users hardly interact with anymore, but still contain huge amounts of personal data. In addition, Meta said it could collect addition information from any third party and scrape data from online sources. Only personal chats between individual users had been excluded.

Users haven't been given any information about the purpose of Meta's AI technology, which is against the requirements of the GDPR. The company's privacy policy would have theoretically allowed for any purpose, which is particularly worrying because the change would have involved about 4 billion Meta users around the world.



Normally, the processing of personal data in the European Union is illegal by default. Therefore, Meta must rely on one of the six legal bases under Article 6(1) GDPR in order to process personal data. Although the logical choice would be to ask for opt-in consent, Meta claimed that it has a "legitimate interest" that overrides the fundamental rights of users. Meta has previously argued this in the context of using all personal data for advertising – and was rejected by the Court of Justice (see C-252/21). Meta used the same legal basis to justify an even broader and more aggressive use of people's personal data.

Complaints filed. On 6 June 2024, noyb filed complaints in 11 European countries, asking the competent data protection authorities to launch an urgency procedure to stop this change immediately, before it would have come into force on 26 June 2024.

Results. Just eight days later, on 14 June 2024, the Irish Data Protection Commissioner (which is the competent authority for Meta) announced that Meta has committed that it won't process EU/EEA user data for its undefined artificial intelligence systems. Even though the authority didn't provide further context or information about its engagement to stop Meta's AI plans, the obvious explanation would be that after 11 complaints by *noyb* and other organisations (such as the Norwegian Consumer Council) with various DPAs in Europe, and public reactions by EU/EEA DPAs in response to these complaints, the pressure on the DPC increased.

3.1.1.2 Complaints against Twitter's AI plans

Background. Despite Meta's failure, Twitter (now X) began unlawfully using the personal data of more than 60 million European users to train its own AI technologies shortly after. Unlike Meta, Twitter did not even inform its users in advance. On the contrary, it seems that most people found out about the new default setting through a viral post on 26 July 2024 - over two months after the AI training had begun.

Twitter's attempt to ingest the data of all EU/EEA users into its AI systems prompted an unexpected response by the Irish DPC: The authority took court action against Twitter to stop the illegal processing and enforce an order to bring its systems into compliance with the GDPR.

Unfortunately, it quickly became clear that the DPC would just settle with Twitter via a so-called undertaking to pause the training of the algorithm with EU data – without tackling the core violations.

The undertaking only says that data that has been processed for AI purposes "between May 7, 2024 and August 1, 2024, shall be deleted and not processed". Conversely, this means that Twitter has by no means stopped using EU/EEA data for its artificial intelligence systems without consent after August 1, 2024.

Complaints filed. As the limited scope of the undertaking already became clear during the first court hearing, *noyb* decided to file complaints against Twitter's practices in 9 EU Member States to involve as many data protection

authorities as possible – and to ensure that the core violations are being investigated.

Current state of the case. The case is still ongoing and lies with the Irish DPC. In December 2024, the authority rejected *noyb*'s request for access to the case file and informed us that it would only start engaging with *noyb* after a preliminary assessment of the matter.

3.1.1.3 Complaint against ChatGPT's lack of data accuracy

Background. The launch of ChatGPT in November 2022 triggered an unprecedented AI hype. People started using the chatbot for all sorts of purposes, including research tasks. The problem is that, according to OpenAI itself, the application only generates "responses to user requests by predicting the next most likely words that might appear in response to each prompt". While the company has extensive training data, there is currently no way to guarantee that ChatGPT is actually showing users factually correct information. Instead, OpenAI simply argues that "factual accuracy in large language models remains an area of active research".

EU law requires that personal data must be accurate. This principle is enshrined in Article 5 GDPR. Individuals also have a right to rectification under Article 16 GDPR if data is inaccurate, and can request that false information is deleted. In addition, under the "right to access" in Article 15, companies must be able to show which data they hold on individuals and what the sources are.

This is very much a structural problem for providers of LLMs. According to a New York Times report, "chatbots invent information at least 3 percent of the time – and as high as 27 percent". This happened to the complainant (a public figure) in our case against OpenAI. When asked about his birthday, ChatGPT repeatedly provided incorrect information instead of telling users that it doesn't have the necessary data.

Despite the fact that the complainant's date of birth provided by ChatGPT is incorrect, OpenAI refused his request to rectify or erase the data, arguing that it wasn't possible to correct data. OpenAI says it can filter or block data on certain prompts (such as the name of the complainant), but not without preventing ChatGPT from filtering all information about the complainant. OpenAI also failed to adequately respond to the complainant's access request. Although the GDPR gives users the right to ask companies for a copy of all personal data that is processed about them, OpenAI failed to disclose any information about the data processed, its sources or recipients.

Complaint filed. On 29 April 2024, *noyb* has therefore filed a complaint with the Austrian data protection authority (DSB), asking for a full investigation of OpenAI's data processing and the measures taken to ensure the accuracy of personal data processed in the context of the company's large language models. Furthermore, *noyb* asks the DSB to order OpenAI to comply with the complainant's access request and to bring its processing in line with the GDPR. Last but not least, *noyb* requests the authority to impose a fine to ensure future compliance.

Current state of the case. The Austrian data protection authority has forwarded the complaint to the Irish Data Protection Commission (DPC), where the complaint is still pending.

3.1.2 Credit Referencing

In some European countries such as Germany and Austria, credit referencing agencies play a pivotal role in assessing individuals' creditworthiness. These companies process vast amounts of personal and financial data to calculate scores that are then sold to their customers. This includes online shops, telecommunications providers or energy providers. This extensive data collection practice raises significant data protection concerns, particularly around the transparency regarding data sources, the processing and the accuracy of the scores. In 2024, noyb has filed additional complaints against credit referencing agencies.

3.1.2.1 Complaint against SCHUFA

Background. Anyone looking for a flat or house to rent in Germany is regularly asked to prove their financial reliability. As a result, people looking for accommodation often end up at credit agencies such as SCHUFA – a company that collects data to calculate credit worthiness and then sells this information. What SCHUFA deliberately conceals: according to Article 15 GDPR, it would have to provide all data free of charge and without undue delay. This should not only include a copy of a person's data, but also the purpose of the processing, the categories of data that are processed, information about the recipients, the data sources and duration of storage.

On its website, SCHUFA only advertises its so-called "BonitätsAuskunft" for €29.95 to private individuals and claims that it offers an "advantage on the housing market". A transparent reference to the Article 15 GDPR right to free information is not provided. The vast majority of data subjects is unlikely to even find the free information. Although the GDPR stipulates that companies must support data subjects in obtaining their free information, SCHUFA does not even mention it by name. The company casually refers to the information in accordance with Article 15 GDPR as a "data copy". In fact, a range of further information needs to be included as well.

Complaint filed. noyb has therefore filed a complaint against SCHUFA with the Hessian data protection authority on 16 February 2024. By systematically hiding and delaying the free information and deliberately withholding data, the company is in breach of the GDPR. In addition, noyb is filing a report with the Hessian DPA. SCHUFA systematically violates the legal requirement of free information by creating the impression that only the paid products are suitable as proof to third parties.

Current state of the case. The complaint is still pending with the Hessian data protection authority.

3.1.2.2 Complaint against KSV1870 for automated decision making

Background. When attempting to conclude a contract with the energy provider Unsere Wasserkraft, new customers are subjected to a fully automated credit check by the credit reference agency KSV1870. Customers are not asked for their consent to this data processing. If someone is assigned a supposedly insufficient score, they are automatically rejected by Unsere Wasserkraft without any further verification measures.

What makes this procedure so problematic is that the decision was fully automated. This means that at no point were people involved who could have pointed out possible errors. The GDPR makes it unmistakably clear that fully automated decisions with such far-reaching effects (with a few exceptions) are generally prohibited.

In the meantime, the European Court of Justice (CJEU) has also ruled that such a procedure is unlawful. In its judgement on a case against the German credit reference agency SCHUFA, the CJEU stated: If companies use the

result of a credit check as a decisive factor for decisions, this credit check alone is considered a fundamentally prohibited decision in accordance with Article 22 GDPR.

Nevertheless, KSV1870 falsely claims that the calculated creditworthiness values have no significant influence on the decisions of companies that use precisely this score. As a reminder: Unsere Wasserkraft rejected the complainant solely on the basis of KSV's credit assessment. There was no manual review of the application. Instead of providing legally compliant measures, the companies are blaming each other: KSV 1870 believes that its cooperation partners must check individual cases, but they in turn refer their customers to KSV.

Complaint filed. On 29 August 2024, noyb has therefore filed a complaint against the credit reference agency KSV1870 and against the energy provider Unsere Wasserkraft with the Austrian data protection authority (DSB). The companies have violated Articles 13, 14, 15 and 22 GDPR. noyb is calling on the DPA to impose a processing ban on KSV with regard to the automatic calculation of creditworthiness scores as long as it is not ensured that these assessments are limited to the few authorised individual cases.

Current state of the case. The complaint is still pending with the Austrian data protection authority.

3.1.3 Data Subject Rights

Under the GDPR, data subjects are granted a comprehensive set of rights designed to give them control over their personal information. These rights include among others the access to their data, the ability to correct inaccuracies and the right to erasure. Despite clear legal obligations, many companies violate these rights, whether by failing to respond to data access requests within the mandated time frame or making it difficult for users to delete or rectify their information. *noyb* has filed several complaints for affected users.

3.1.3.1 Complaint against BeReal

Background. The concept of BeReal as a social media platform is simple: Every day, users receive a randomly timed notification to take a photo with their smartphones' front and rear camera within the next two minutes. Only then are they allowed to see what their friends are up to. This is supposed to guarantee that people give a "real" insight into their daily lives. To date, this attracted more than 23 million daily global users.

With this approach, the app tries to differentiate itself from platforms such as Instagram and Facebook.

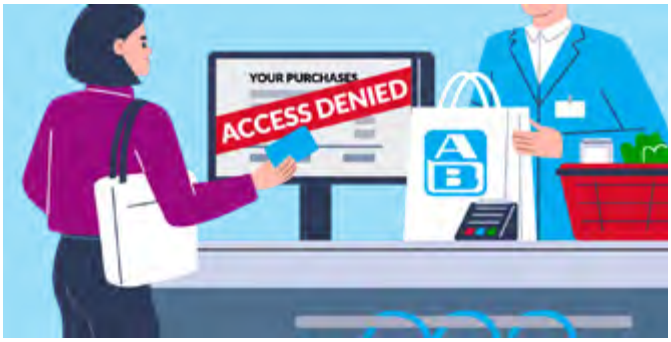
Unfortunately, it also tries to pressure people into being tracked. Since July 2024, European BeReal users have been confronted with a consent banner as soon as they open the app. While at first glance, it appears that users have a convenient choice, it quickly becomes clear that this choice is not intended by BeReal. If you accept the use of your personal data for advertising purposes, you won't see the banner again. If you "refuse", however, the banner will reappear every single day when you try to publish a post. This is a prime example of a so-called dark pattern, designed to manipulate the users' decision and annoy them into consent.

The European Data Protection Board (EDPB) has already addressed dark patterns similar to those used by BeReal in guidelines from 2022. When repeatedly prompted to consent, "users are likely to end up giving

in as they are wearied from having to refuse the request each time they use the platform," the authority writes.

Complaint filed. On 12 December 2024, *noyb* has therefore filed a complaint with the French data protection authority (CNIL). BeReal's daily attempt to pressure its users into accepting the tracking for personalised advertising has a significant impact on user behaviour. Consent given under these circumstances is not freely given, which means it doesn't meet the requirements established in Article 4(11) GDPR and therefore invalid.

Current state of the case. The complaint is still pending with the French data protection authority. On 14 March 2025, the CNIL has informed *noyb* that it is investigating the case.



3.1.3.2 Complaint against Greek supermarket over loyalty cards

Background. To retain as many loyal customers as possible, the Greek supermarket chain Alfa Vita (AB) has introduced a loyalty card programme called "AB plus". Unfortunately, its compliance with EU law is lacking. This became clear when a consumer tried to exercise her right of access. She is registered to the AB Plus Personal tier of AB's loyalty programme. This means that AB processes "their buying habits, the frequency of their visits to an AB store, the use of offers communicated to them, their home address, the total cost of their purchases" for profiling. Still, AB only provided her with a list of her transactions and her contact details, but no other information that it has derived from it. Despite a clear Court of Justice ruling, AB has also explicitly refused to provide a list of recipients of such data. (see case C-154/21).

AB Plus Personal customers, including the complainant, can't even access the amount of money they have saved by using their loyalty card. On its website, AB advertises access to this data as an exclusive feature for "AB Plus Unique" customers. However, an "upgrade" to AB Plus Unique would require consent to the sharing of data with other third parties.

Complaint filed. On 13 August 2024, *noyb* has therefore filed a complaint with the Greek data protection authority, requesting an investigation of AB's processing operations and an order to comply with the complainant's access request. In addition, *noyb* suggests the DPA to impose a fine of up to 4% of AB's annual turnover to prevent similar violations in the future.

Current state of the case. The complaint against Alfa Vita is still pending with the Greek data protection authority, which is actively investigating the case.

3.1.3.3 Xandr granting GDPR rights at rate of 0%

Background. If companies want to use targeted advertising to promote their products or services online, they have to go through so-called Real Time Bidding (RTB) platforms. One such platform is run by Microsoft subsidiary Xandr, which allows advertisers to buy ad space on websites or in mobile apps in a fully automated way. When a user visits a website, an algorithmic auction takes place in order to decide which company can display an advertisement.

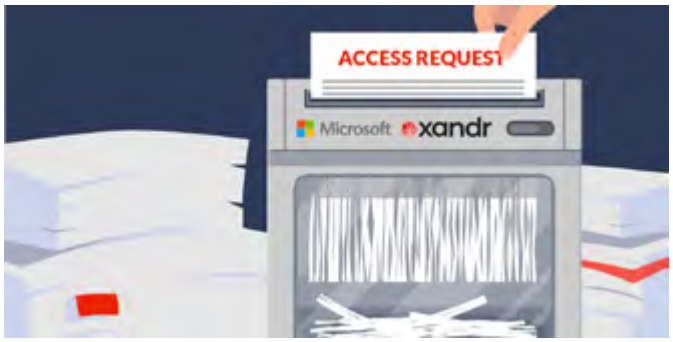
Because a users' interests and characteristics ultimately determine an advertiser's willingness to place an ad, Xandr collects and shares a massive amount of personal data in order to profile the users and to allow for targeting.

According to the GDPR, everyone has the right to get access to their information. However, Xandr reports an astonishing 0% response rate to access and erasure requests in 2022. The complainant has experienced this approach first hand: When he requested access to his data, Xandr claimed that it couldn't identify him - and denied his request for access and erasure. In reality, the

company has all the necessary information to single out specific data subjects. Identifying and targeting individuals is after all their core business. In addition, the GDPR requires data about individuals to be 'accurate'. However, the available information suggests that Xandr's system uses tons of false information about users.

Complaint filed. On 9 July 2024, *noyb* has therefore filed a complaint against Xandr with the Italian data protection authority (Garante) regarding transparency issues, the right of access and the use of inaccurate information about users. Overall, Xandr appears to be in breach of Article 5(1)(c) and (d), Article 12(2), Article 15 and Article 17 of the GDPR.

Current state of the case. The complaint is still pending with the Italian data protection authority. On 10 February 2025, the Garante confirmed that it is investigating the case.



3.1.4 Online Tracking

When you use the Internet, you are inevitably confronted with tracking. Most websites and apps place tracking cookies to monitor your behaviour and show you advertising based on your interests. In many cases, this happens without companies ever asking for people's consent. To combat this approach, *noyb* filed several new complaints dealing with invasive online tracking.

3.1.4.1 Microsoft in Schools

Background. In the wake of the pandemic, schools in the European Union have increasingly begun to implement digital services for online learning. While these

modernisation efforts are a welcome development, a small number of big tech companies immediately tried to dominate the space – often with the intention of getting children used to their systems and creating a new generation of future "loyal" customers. One of them is Microsoft, whose 365 Education services are widely used.

Microsoft tries to dodge responsibility by insisting that almost all of it lies with local authorities or schools. In reality, neither has the power to influence how Microsoft actually processes user data. Instead, they are faced with a take-it-or-leave-it situation where all the decision-making power and profits lie with Microsoft. Schools have no realistic way of negotiating or changing the terms. This leads to a situation where Microsoft is trying to contractually dump most of its legal responsibilities under the GDPR on schools that provide Microsoft 365 Education services to their students. This means, for example, that access requests to Microsoft go unanswered - while schools have no realistic way of complying with such requests because they don't hold the necessary data.

Trying to find out exactly the exact privacy policy or the documents that apply to the use of Microsoft 365 Education is an expedition in itself. There is a serious lack of transparency, forcing users and schools to navigate a maze of privacy policies, documents, terms and contracts that all seem to apply. But this is not the only issue at hand. Although the complainant did not consent to tracking, Microsoft 365 Education still installed cookies that, according to Microsoft's own documentation, analyse user behaviour, collect browser data and are used for advertising. Such tracking, which is commonly used for highly-invasive profiling, is

apparently carried out without the complainant's school even knowing.

Complaint filed. On 4 June 2024, *noyb* has therefore filed two complaints against Microsoft. Neither Microsoft's privacy documentation, requests for access, or *noyb*'s own research could fully clarify this, which violates the GDPR's transparency provisions. In addition, the company failed to comply with the right of access. As the terms and conditions and the privacy documentation of Microsoft 365 Education are uniform for the EU/EEA, all children living in these countries are exposed to the same violations of their GDPR rights.

Current state of the case. Both complaints are still pending with the Austrian data protection authority, which is actively investigating the case.

3.1.4.2 Complaint against Pinterest

Background. More than 130 million people in the European Union currently use Pinterest. The image and video-based social media platform allows users to search for all sorts of different topics, be it home decor, food recipes, fashion or travel tips. As with most social media platforms, Pinterest is partly funded by personalised advertising. To do this, the company tracks users - without ever asking for their consent, as required by law. Instead of seeking opt-in consent under Article 6(1)(a) GDPR, it falsely claims to have a legitimate interest in processing people's personal data under Article 6(1)(f) GDPR. Tracking is turned on by default and would require an objection (opt-out) by each user to stop.

The complainant only found out about Pinterest's ad tracking by chance. After using the platform for some time, she checked the "privacy and data" settings and found out that the "ads personalisation" was turned on by default. According to these settings, Pinterest uses information from visited websites and from other third parties to show users personalised ads. In addition, Pinterest tracks on-site activity "to improve the ads about Pinterest you're shown on other sites or apps."

This practice is clearly unlawful since the introduction of the GDPR in 2018. In its ruling in case C252/21 Bundeskartellamt in 2023, the Court of Justice of the European Union (CJEU) found again that personalised advertising cannot be based on legitimate interest under Article 6(1)(f) GDPR.

Complaint filed. On 22 October 2024, *noyb* has therefore filed a complaint against Pinterest with the French data protection authority (CNIL). Pinterest violated Article 6(1) GDPR by processing the complainant's personal data for personalised advertising on the basis of legitimate interest. Pinterest also violated Article 15(1)(c) GDPR by failing to provide access to the categories of data that were shared with third parties.

Current state of the case. The case is still pending with the French data protection authority, which, in July 2025, has refused to grant *noyb* access to the letter it has sent to Pinterest. The case is still under investigation.

3.1.4.3 Tracking in the Firefox browser

Background. When it updated Firefox last summer, Mozilla has secretly enabled a so-called Privacy Preserving Attribution (PPA) feature, without informing its users. Similar to Google's (failed) Privacy Sandbox, this turned the browser into a tracking tool for websites. Instead of placing "traditional" tracking cookies, websites have to ask Firefox to store information about people's ad interactions in order to receive the bundled data of multiple users.

Mozilla claimed that the development of the Privacy Preserving Attribution improves user privacy by allowing ad performance to be measured without individual websites collecting personal data. In reality, part of the tracking is now done directly in Firefox. While this may be less invasive than unlimited tracking, which is still the

norm in the US, it still interferes with user rights under the EU's GDPR. In reality, this tracking option doesn't replace cookies either, but is simply an alternative - additional - way for websites to target advertising.

Furthermore, Mozilla has turned on its Privacy Preserving Attribution by default. Users have not been informed about this move, nor have they been asked for their consent to be tracked by Firefox. The feature wasn't even mentioned in Mozilla's data protection policies.

Complaint filed. On 25 September 2024, *noyb* has therefore filed a complaint with the Austrian data protection authority (DSB). Mozilla should properly inform the complainant and other users about its data processing activities – and effectively switch to an opt-in system. In addition, the company should delete all unlawfully processed data.

Current state of the case. The complaint against Mozilla is still pending with the Austrian data protection authority, which is actively investigating the case.

3.1.4.4 Tracking in Google Chrome

Background. After years of growing criticism over invasive ad tracking, Google announced in September 2023 that it would phase out third-party cookies from its Chrome browser and introduced a supposed "ad privacy feature". While the so-called Privacy Sandbox is advertised as an improvement over extremely invasive third-party tracking, the tracking is now simply done within the browser by Google itself. To do this, the company theoretically would have needed the same informed consent from users. Instead, Google has been tricking people by pretending to "Turn on an ad privacy feature".

Google's internal browser tracking was introduced to users via a pop-up that said "turn on ad privacy feature" after opening the Chrome browser. In the European Union, users are given the choice to either "Turn it on" or to say "No thanks", so to refuse consent. In a letter to *noyb*, Google argued that choosing to click on "Turn it on" would indeed be considered consent to tracking under Article 6(1)(a) of the GDPR. In reality, the company concealed the fact that selecting this option would turn on first-party tracking.

Similar to Mozilla, Google's main argument is that the new Privacy Sandbox is less invasive than third-party tracking systems. While this may be true, it does not mean that Google can do whatever it wants without complying with European data protection law.

Complaint filed. On 13 June 2024, *noyb* has therefore filed a complaint with the Austrian data protection authority (DSB). Article 4(11) of the GDPR clearly states that consent must, among other things, be a "specific, informed and unambiguous indication of the data subject's wishes". Given the highly misleading pop-up banner, the complainant had no way of knowing that he was actually consenting to the processing of his data for targeted advertising.

Current state of the case. The complaint against Google is still pending with the Austrian data protection authority.

3.1.5 Other enforcement actions

3.1.5.2 Taking the Swedish DPA to court over inactivity

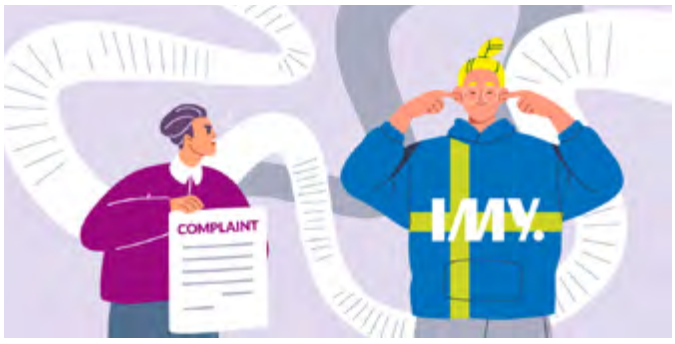
Background. Contrary to EU law, the Swedish Data Protection Authority (IMY) regularly refuses to properly handle complaints from data subjects. Even after a ruling by the Supreme Administrative Court of Sweden, the IMY frequently just forwards a complaint to the

company that illegally processes personal data - and then immediately closes the case without investigating. However, the GDPR clearly stipulates that authorities must not only process each and every complaint, but also remedy the situation.

The IMY's way of dealing with complaints since the Supreme Administrative Court ruling is to attach an "appeal form" to their (non-)decisions. But it still doesn't investigate the complaints. Instead, the authority simply forwards the complaint to the entity that illegally processes personal data and then immediately closes the case. This also happened in the case preceding *noyb*'s current legal action against the IMY. After a data subject filed a complaint regarding a recorded phone call, the authority forwarded it to the respondent without investigating.

In several cases (see C-311/18, C-26/22 and C-64/22), the European Court of Justice has clearly stated that every data protection authority must handle the complaint with due diligence. Surprisingly, the Swedish first instance court (Förvaltningsrätten i Stockholm) has still agreed with the IMY's approach.

Appeal filed. On 8 August 2024, *noyb* has therefore filed an appeal with the second instance court (Kammarrätten i Stockholm) to ensure that the right to have every complaint properly handled is also enforced in Sweden.



3.1.5.3 Swedish data brokers (MrKoll)

Background. While Article 85 of the GDPR allows member states to limit the application of some elements of the GDPR in the area of journalism (to e.g. protect sources or undercover investigations), Sweden

took a brute force approach to this exception. Swedish national legislation makes it extremely easy to obtain a "media licence", even if a company's activities are not even remotely related to those of a news outlet. In Sweden, anyone can get a media license and become exempt from the GDPR.

Even data brokers, meaning privately operated companies that buy and sell the personal data of millions of people without their knowledge, can use this loophole to exempt themselves from any obligations under the GDPR. This deprives the people of their fundamental right to privacy and exposes their most intimate data to the internet.

One of Sweden's largest data brokers, MrKoll, illustrates this issue very well. The company has data on almost the entire Swedish population and makes a profit by selling it to anyone who's interested without a single safeguard or restriction. The data sold includes not only people's names, surnames, dates of birth, telephone numbers, home and work addresses. The company also has data on real estate values, the car they drive, pending civil proceedings, penalties, criminal records and detailed case records. Almost all of the information is provided directly by the Swedish authorities. There is even a list of the most searched for people on the data broker's website.

Contrary to Article 17 GDPR, which usually gives everyone a right to object to the use of their personal data, there is currently no way to have your data deleted from MrKoll's website. The complainant's request to have his data deleted was rejected on the grounds that "the database is not affected by the General Data Protection Regulation (GDPR)" because of MrKoll's media license.

Complaint filed. On 14 March 2024, *noyb* has therefore filed a complaint against MrKoll with the Swedish data protection authority (IMY). MrKoll has refused the complainant's request to delete his data, thereby violating his rights under Article 17 GDPR.

Current state of the case. The complaint against MrKoll is still pending with the Swedish data protection authority, which has initiated an investigation.

3.1.5.4 EU Parliament data breach

Background. In early May 2024, the European Parliament informed its staff of a massive data breach in the institution's recruiting platform. The breach affected the personal data of more than 8,000 staff. This included ID cards and passports, criminal record extracts, residence documents and even sensitive data such as marriage certificates that reveal a person's sexual orientation. The Parliament only found out about the breach months after it happened, and still doesn't seem to know the cause.

This incident is particularly worrying, because the Parliament has long been aware of cybersecurity vulnerabilities: In November 2023, the Parliament's IT department conducted a cybersecurity review – and concluded that the institution's cybersecurity "has not yet met industry standards" and that existing measures were "not fully in-line with the threat level" posed by state-sponsored hackers.

The data breach also reveals that the Parliament isn't complying with the GDPR's data minimization and retention requirements. Article 4(1)(c) EU GDPR requires EU institutions to only process data that is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Nevertheless, the EU Parliament's retention period for recruitment files is 10 years.

Complaint filed. On 22 August 2024, *noyb* has therefore filed two complaints against the European Parliament with the European Data Protection Supervisor (EDPS). The EU Parliament appears to have breached Articles 4(1)(c) and (f) and 33(1) of the EU GDPR. Additionally, in one complainant's case, the Parliament refused an erasure request made after the breach, citing the 10-year retention period, despite the complainant's concerns given the breach and fact that they had not worked there for several years.

Current state of the case. Both complaints are still pending with the European Data Protection Supervisor. The authority has confirmed the receipt of the complaints on 26 August 2024.

3.1.5.5 Complaint against Austrian news site Kurier

Background. On 5 June 2024, *noyb* has filed another complaint against the Austrian newspaper Kurier. Before implementing a "Pay or OK" system, the newspaper had forced its users to consent to Google and other tracking cookies when visiting its website. In doing so, the company clearly violated the GDPR, a fact that was also confirmed by the Austrian data protection authority: The latter had already banned the news magazine Profil (which is part of the same media group) from using such forced consent. The system has since been changed. Users now have the option to consent or signing up to a paid subscription (Pay or Okay).

This is not the first time the Austrian data protection authority (DSB) has been confronted with this violation. *noyb* has filed a complaint concerning an almost identical forced banner on profil.at in 2022. Back then, the DSB ordered the news magazine to adapt its website and obtain legally compliant consent. This never happened. Instead, the Kurier media group, to which both Profil and Kurier belong, decided to extend its practice to kurier.at and challenge the authority's decision.

Current state of the case. On 20 August 2024, the DSB decided that Kurier did indeed process personal data unlawfully. Kurier has appealed the decision at the Bundesverwaltungsgericht. There's no final court judgement yet.

3.1.5.6 *noyb*'s second complaint against Ryanair

Background. Whoever wants to book a flight on the Ryanair website or app is forced to create a permanent account. This often means that data is combined and kept until you delete the account. However, an account is clearly not necessary to book a flight. In reality, Ryanair's forced accounts violate the GDPR's data minimization principle. Article 5(1)(c) GDPR requires that personal data should only be processed if it is necessary. Ryanair fails to meet this requirement.

In order to fly with Ryanair, all new account owners must go through a mandatory 'verification' process. At this point, people can theoretically choose between two options. In reality, Ryanair nudges them towards a pre-selected and highly invasive biometric facial recognition process to verify their account - despite biometric data being specially protected by EU law. European Data Protection Authorities even say that facial recognition can pose "unacceptably high risks" to people.

If customers don't want their biometric data to be processed, Ryanair requires them to send them a hand-written signature and a copy of their government ID. This creates an additional burden for refusing consent to the use of their biometric data, leading to customers being robbed of their free choice – and Ryanair not complying with the consent requirements of the GDPR.

Complaint filed. On 19 December 2024, *noyb* has therefore filed a complaint with the Italian data protection authority (Garante). By forcing users to create an account to buy a plane ticket, the airline violates the data minimisation principle according to Article 5(1)(c) GDPR. In addition, the mandatory verification violates the purpose limitation principle (Article 5(1)(b) GDPR). Last but not least, Ryanair fails to meet the consent requirements in accordance with Articles 6 and 9 GDPR.

Current state of the case. The Italian data protection authority has forwarded the complaint to the Irish DPC. The case is still pending.

3.2. 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. In 2024, we also published our first DPO report, analysing how privacy professionals see GDPR enforcement from within companies. In addition, we published a consent banner report to see how data protection authorities actually decide in cases concerned with questionable cookie banner designs.

3.2.1. 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 2024, the number of decisions collected and summarised has grown to more than 4,100, with more than 12,000 subscribers to the weekly GDPRtoday newsletter. More than 230 active volunteers help *noyb* to collect and summarise these decisions in jurisdictions *noyb* could never cover in-house due to language barriers.

3.2.2. Consent Banner Report

How authorities actually decide. Following several hundred *noyb* complaints against companies that use questionable consent banners, the European Data Protection Board established a "cookie banner taskforce" in September 2021. In January 2023, the taskforce then published a report offering its opinion and recommendations regarding the different kind of violations found in consent banners.

With its new Consent Banner Report, *noyb* has compared the EDPB taskforce's findings for each consent banner violation with the positions taken by national DPAs in guidance documents and actual decisions. We believe that this report will be a valuable resource for companies setting up consent banners. In addition, we hope that the report will spark further discussion about the guidelines adopted on deceptive practices, and how they can be developed in the future to ensure that users have a fair and free choice in consent banners.

The report addresses different practices in turn, outlining some of the relevant issues, the position of the EDPB taskforce, and the guidelines published by national DPAs. Where available, information on actual DPA decisions will be added.

3.2.3. Report on GDPR (non)-compliance

Survey among privacy professionals. When the GDPR came into force in 2018, the new data protection law was hailed as a shift towards stricter enforcement – ensuring that in the EU, the fundamental right to data protection does not only exist on paper. In an attempt to move towards "evidence-based enforcement", *noyb* conducted a survey among more than 1000 data protection professionals working in European companies to learn which factors impact (non-) compliance in companies. Most respondents see serious problems. This provided a unique view from the inside: 70% of respondents believe that authorities need to issue clear decisions and enforce the GDPR to ensure compliance, while 74% say that authorities would find 'relevant violations' if they would walk through the door of an average company. The report also shows that authorities would need to fundamentally change their approach to enforcement to get businesses to comply.

→ You can read the report here.

3.3. Updates on ongoing projects

Due to the large number of pre-existing and pending cases, this chapter only reports on cases with significant developments in the course of 2024. This can be a court ruling, a DPA decision, an administrative fine or an appeal.

3.3.1. CJEU decision: Meta must minimise use of personal data

Data use must be minimised. In its ruling (C-446/21) on 4 October 2024, the European Court of Justice (CJEU) has fully backed a lawsuit brought against Meta over its Facebook service. The CJEU decided on two questions. With this, it massively limits the use of personal data for online advertising. It has also limited the use of publicly available personal data to the originally intended purposes for publication.

Background on first question. So far, Meta has used all the personal data it has ever collected for advertising. To prevent such practices, the GDPR established the principle of data minimisation in Article 5(1)(c) GDPR, requiring to limit the processing to strictly necessary data. Meta and many other players in the online advertising space have simply ignored this rule and did not foresee any deletion periods or limitation based on the type of personal data.

But the data minimisation principle radically restricts the use of personal data for advertising, and it applies regardless of the legal basis used for the processing. Even a user who consents to personalised advertising cannot have their personal data used indefinitely. In line with the common practice of the CJEU, the Court left the details of how to implement the data minimisation principle to the national courts.

Background on second question. Under Article 9(2)(e) GDPR, information that is "manifestly made public" may be processed by a company, because the legislator assumes that the data subject agreed to the use. Mr Schrems argued that his public comments were made years after the processing of other information took place. His later comments could not be seen as an agreement to the processing of other information years ago and cannot have "travelled" back in time. Other parties to the procedure also questioned, if the mere mention of a fact during a public discussion would amount to making such information manifestly public.

3.3.2. Long back and forth with cookie complaints in Belgium

Going on for a long time. In July 2023, *noyb* has filed 15 complaints against Belgian news sites using deceptive cookie banners with the Belgian DPA. 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.

In September 2024, the Belgian data protection authority then ordered four of the news sites to bring their cookie banners into GDPR compliance. Specifically, De Standaard, Het Nieuwsblad, Het Belang van Limburg and Gazet van Antwerpen were ordered to add a “reject” button to the first layer of their cookie banners. In addition, the news sites have been ordered to change the currently misleading colour scheme of the buttons used.

The controller appealed the DPA’s decision in 2024. In March 2025, the Brussels Market Court annulled the decision. Our complaint against RTL Belgium had the same outcome. After *noyb* had won the case before the data protection authority, the Market Court annulled its

decision in early 2025.

The remaining cases. The *noyb* complaints against three news outlets managed by the IPM Group have been resolved via a settlement. To date, the controller hasn't complied with the settlement agreement.

The *noyb* complaints against VRT, Mediafin and RTBF have been resolved via a settlement as well. All three companies now comply.

3.3.3. Norwegian court confirms Grindr fine

On 1 July 2024, The Oslo District Court in Norway has confirmed that Grindr has violated the GDPR by sharing user data with advertisers. This also confirmed that Grindr must pay a fine of NOK 65 million, which translates to € 6.65 million.

The case was based on a complaint by the Norwegian Consumer Council (Forbrukerrådet) in Summer 2024 and was supported by *noyb*.

3.3.4. German DPA declares data trading between CRIF and Acxiom illegal

Case won. In early February 2024, noyb has scored a stage victory in its proceedings against the credit reference agency CRIF and the address trader Acxiom in Germany. The companies are illegally trading the personal data of millions of Germans. On 18 October 2021, *noyb* therefore filed a complaint. Now the Bavarian data protection authority has ruled that CRIF has misused the purchased data – and therefore violated European data protection law. Meanwhile, the Hessian authority has rejected an application by Acxiom to deny *noyb* any access to the case files.

3.3.5. Campaign to stop Pay or OK on Meta platforms

Background. In November 2023, Meta adopted a Pay or OK system. Since then, users are forced to choose between paying a monthly fee or being tracked for personalised advertising. On 26 January 2024, The Dutch, Norwegian and Hamburg data protection authorities (DPAs) have therefore requested a binding opinion by the European Data Protection Board (EDPB) on this matter.

Shortly after, on 16 February 2024, noyb joined forces with 27 other NGOs (including Wikimedia Europe, Bits of Freedom and the Norwegian Consumer Council) to urge the EDPB to issue an opinion that protects the fundamental right to data protection.

In reality, most people simply have no choice but to accept the exploitation of their data, when confronted with a fee. The effect is clearly illustrated by scientific studies: For example, the CEO of the "Pay or Okay" provider contentpass stated that 99.9 % of visitors agree to tracking when faced with a € 1.99 fee. At the same time, objective surveys suggest that only 3-10 % of users want their personal data to be used for targeted advertising.

First opinion. On 17 April, the EDPB then published its first opinion on Pay or OK in relation to large online platforms such as Instagram and Facebook.

"In most cases, it will not be possible for large online platforms to comply with the requirements for valid consent if they confront users only with a binary choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee," the EDPB wrote.

According to the EDPB, users should be offered a third alternative, "free of charge, without behavioural advertising, e.g. with a form of advertising involving the processing of less (or no) personal data."

General guidelines are being worked on. The EDPB is currently working on more general guidelines for Pay or OK that will be valid for all companies and not only large online platforms.

3.3.6. €4.75 Million fine for Netflix

Background. In January 2019, *noyb* filed eight complaints against a series of streaming providers such as Amazon, Apple Music, Spotify, YouTube – and Netflix. All of these companies failed to adequately respond to users' access requests under Article 15 GDPR in one way or another. According to the right of access, companies are obliged to grant their users access to a copy of all raw data that it about the user, as well as additional information about the sources and recipients of the data, the purpose for which the data is processed or information about the countries in which the data is stored and how long it is stored.

Decision in favour of the data subject. On 18 December 2024, the Dutch data protection authority has sided with *noyb* and found that Netflix didn't provide its customers clear enough information about what it exactly does with their data. Netflix was fined €4.75 million. While the decision highlights a number of important issues with Netflix's handling of access requests, it unfortunately leaves out one important point that was mentioned in *noyb*'s complaint: Netflix didn't just fail to provide sufficient information about why it collects data and what it does with it. The company didn't even manage to provide a full copy of the complainant's data.

According to the DPA, Netflix has already objected to the fine, but hasn't yet appealed the decision as a whole. In the meantime, *noyb* is still waiting for a decision from the Austrian data protection authority (DSB) in the same case against Netflix.

3.3.7. EU Commission microtargeting illegal

Background. In the contentious fight over the heavily criticised chat control regulation (a proposed EU law that could undermine all encrypted online communication to allow authorities to read online chats), the European Commission wanted to politically influence people living in the Netherlands. In an attempt to "flip" the views in the Netherlands, the Commission went to X/Twitter and made posts indirectly promoting this regulation.

However, the European Commission did not only post these political messages, but also targeted users who weren't interested in keywords like: #Qatargate, brexit, Marine Le Pen, Alternative für Deutschland, Vox, Christian, Christian-phobia or Giorgia Meloni. The clear intention was to only target politically liberal or left users, but not conservative or right-wing users. Advertisers often use so-called "proxy data" (so data

closely associated with political thinking) to target political views. By doing so, the European Commission has clearly triggered the processing of personal data of EU citizens to target them with ads.

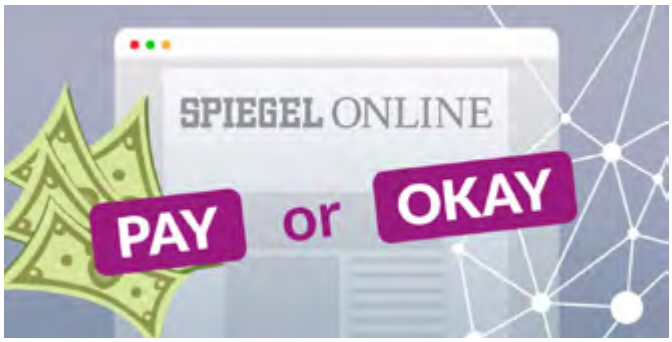
On 16 November 2023, *noyb* had therefore filed a complaint against the EU Commission with the European Data Protection Supervisor (EDPS), which is responsible for EU institutions.

EDPS Decision. On 13 November 2024, the EDPS issued a decision finding that the European Commission has illegally targeted advertising at citizens using sensitive personal data on their political views. The EDPS clarified that the Commission was a controller of the processing operation and is fully liable for unlawful targeting on the platform. However, the online platform may also be held responsible for the same case. *noyb* has also filed a complaint against X/Twitter with the Dutch DPA in 2023.

The EDPS only issued a reprimand - so a formal finding that the processing was illegal and a formal warning. The EDPS considered that other measures, such as a fine, were not necessary as the Commission stopped the practice. The decision was issued under Regulation (EU) 2018/1725, often called the "EU GDPR" that only applies to the EU institutions, but is very similar to the "normal" GDPR that applies to everyone else.

3.3.8. Lawsuit against Hamburg DPA

Background. In the summer of 2021, *noyb* had filed a GDPR complaint against the Pay or OK banner on the website of DER SPIEGEL. At the time, the complainant (and all other users) had to decide whether to allow the news magazine to use personal data or to pay for a subscription. The authority then took almost three years to determine that it considered 'Pay or OK' to be

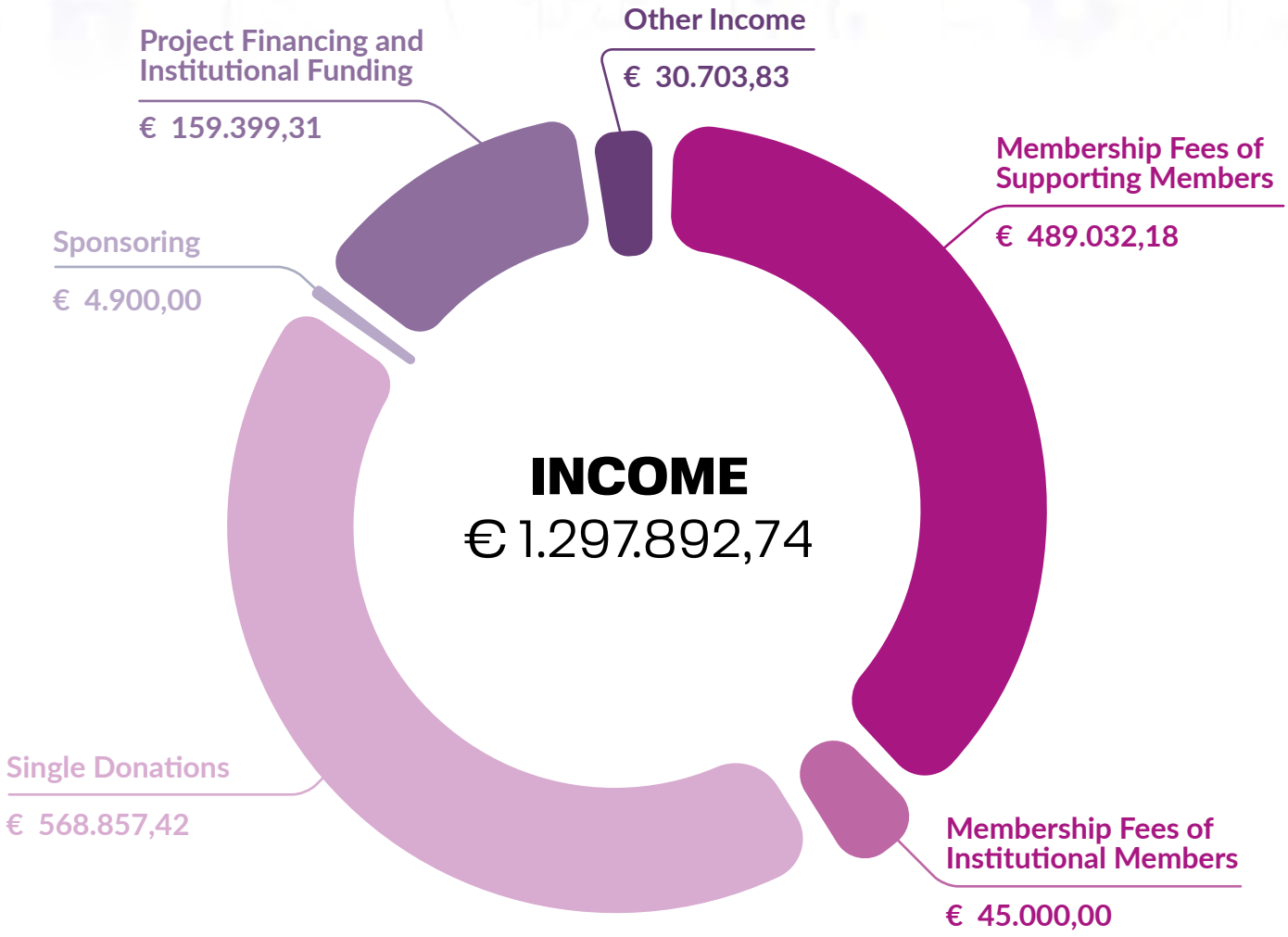


permissible in principle. However, there is no serious discussion of the facts in the decision. There is no justification as to why users having to pay for their basic rights should constitute voluntary consent and genuine freedom of choice. It is known that more than 99.9% agree to tracking when confronted with Pay or OK. Yet only 3-10% actually want personalised advertising. In the meantime, even the EU Commission has expressed considerable doubts about the legality of the model.

The Hamburg DPA was in close contact with SPIEGEL during the proceedings. The authority also met with representatives of the company several times, invited them to its premises and provided feedback on the proposed changes. For the administrative costs of the procedure, the Hamburg authority charged SPIEGEL € 6,140. Another media company had previously even been proactively encouraged by the Hamburg authority to switch to Pay or OK. It can be assumed that the authority actively encourages companies to engage in problematic behaviour. Incidentally, the complainant was only informed of all this after the decision had been made. He was not heard by the authority. The majority of his messages to the authority were not even answered.

Lawsuit against the authority. In August 2021, the complainant has therefore filed a lawsuit with the Hamburg Administrative Court to have the DPA's decision overturned. If this action is successful, the authority would have to decide again on the complaint from 2021.

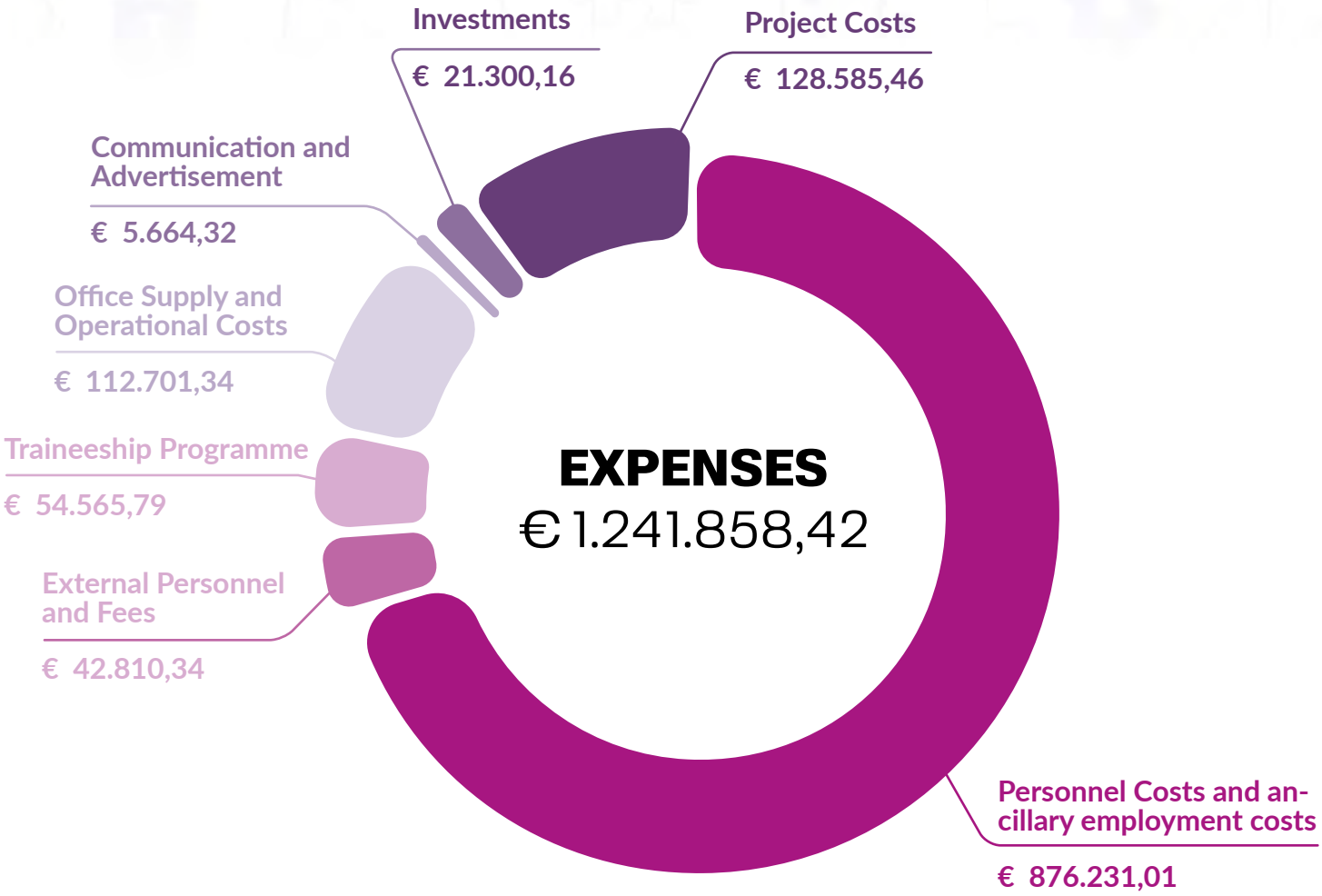
Our finances



- **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**
  donations by individuals and SMEs
- **Sponsoring**
- **Project Financing and Institutional Funding**
  Austrian Ministry for Social Affairs, Sub3, DFF, Luminate
- **Other Income**
  speaking fees, interest

noyb changed from Cashflow Method of Accounting to Balance Sheet Accounting beginning of 2024.

Our finances



- **Personnel Costs and ancillary employment costs**
- **External 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 changed from Cashflow Method of Accounting to Balance Sheet Accounting beginning of 2024.

noyb in the media

TABLE OF CONTENTS

noyb in the media

TABLE OF CONTENTS

noyb in numbers

5 250
Supporting Members

21
Team Members

13
Legal Trainees

36 **Complaints** filed in 2024

498 **Cases** pending

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

> 1.69 billion € in fines

35
Press Releases

11
Newsletters & Member Updates

>78 000
Followers on 6 media platforms

GDPR hub

4 100 Summaries

230 Active Country Reporters

>12 000 Subscribers to GDPRtoday

10 Country Reporter Meetings

*as of Dec 2024

TABLE OF CONTENTS

Thank you for your support
of our work and for the
implementation of data protection!

Institutional Supporters

Bundesministerium
Arbeit, Soziales, Gesundheit,
Pflege und Konsumentenschutz

Stadt Wien

AK WIEN

Sponsors and Partners

dialog Mail eMarketing Systems

DuckDuckGo

Proton Pass

LamaPoll

foundata

freedom internet

LIONWARE

devowl.io

apecdata

noyb **European Center for Digital Rights**

Imprint:
noyb – European Center for Digital Rights

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

ZVR: 1354838270