noyb

European Center for Digital Rights

Annual Report

2025

noyb.eu

Contents

1 PREFACE 4

2 ABOUT *NOYB* 6

2.1 Our Mission 6

2.2 Who we are 6

2.2.1 Organigram and Governance 6
2.2.1.1 Executive Board 7
2.2.1.2 General Assembly 8
2.2.1.4 Staff – Legal Team 9
2.2.1.3 Legal Traineeships 9
2.2.1.5 Staff — Office & Tech Team 10

2.3 How we work 11

2.3.1 Complaints 12
2.3.2 Lawsuits 12
2.3.3 How do we come up with project ideas? 12

3 OUR PROJECTS IN 2025 13

3.1 Enforcement Actions 13

3.1.1 Preparations for a first potential collective redress project 13
3.1.1.1 Over 40,000 CRIF queries: Klarna, banks and telecoms entangled in CRIF network 13

3.1.2 Artificial Intelligence 14
3.1.2.1 Bumble's AI icebreakers are mainly breaking EU law 14
3.1.2.2 AI hallucinations: ChatGPT created a fake child murderer 14
3.1.2.3 Ongoing project against Meta AI 15

3.1.3 First complaints against Chinese tech companies 16
3.1.3.1 TikTok, AliExpress, SHEIN & Co send Europeans' data to China 16
3.1.3.2 TikTok unlawfully tracks people's online behaviour 17

3.1.4 The unlawful use of Europeans' biometric data 17
3.1.4.1 Criminal complaint against facial recognition company Clearview AI 17

3.1.5 *noyb*'s first complaint against a video game company 18
3.1.5.1 Ubisoft unlawfully collects data about your gaming habits 18

3.1.6 Data Subject Rights 18
3.1.6.1 Whitebridge.ai: your personal data is for sale to you and anyone 18
3.1.6.2 WetterOnline sees "disproportionate effort" in complying with the GDPR 19
3.2 Other actions 20
3.2.1 Budget cuts paralyse Austrian DPA: NGO complaint to the EU Commission 20
3.2.2 *noyb* takes Swedish tax authority to court for selling people's personal data 20
3.2.3 Swedbank refuses transparency in automatic interest calculation 21
3.3 Policy work 22
3.3.1 Digital Omnibus 22
3.3.2 GDPR Procedural Regulation 23
3.4 Knowledge Sharing 24
3.4.1 GDPRhub and GDPRtoday 24
3.4.2 Analysis of DPO activities in Europe: Only 1.3 % of cases result in a fine 24
3.4.3 In-depth research into Pay or Okay systems in Europe 25
3.5 Updates on ongoing projects 26
3.5.1 Years of inactivity in "Pay or OK" cases: *noyb* sues German DPAs 26
3.5.2 EU Court: Irish DPC must investigate *noyb* complaint 26
3.5.3 Austrian Supreme Court: Meta must give users full access to their data 27
3.5.4 Conde Nast fined €750,000 for placing cookies without consent 27
3.5.5 Microsoft 365 Education may not track school children 27
3.5.6 Court decides "Pay or Okay" on DerStandard.at is illegal 28
3.5.7 YouTube ordered to honour user's right of access 28
3.5.8 French DPA fines Google €325 million for "Spam Emails" in Gmail 29
3.5.9 Austrian authority forbids unlawful credit scoring by KSV1870 29
4 OUR FINANCES 30
5 *NOYB* IN THE MEDIA 32
6 *NOYB* IN NUMBERS 34

1 Preface

More than 8 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 **€2 billion**, although many of these have not yet been collected due to pending appeals.

While we continued to work on our 460 pending cases, we have also filed 21 new complaints against major companies across Europe in 2025, launched our first collective redress project and invested a lot of time and energy in campaigning against the EU Commission's Digital Omnibus package. Among other things, this allowed us to continue our work in the AI space, to tackle unlawful data transfers to China and to explore new industry branches, including video games.

Among the most significant cases of 2025 is the start of preparations for *noyb*'s **first collective redress case** against the Austrian credit agency CRIF. This project will keep us busy in 2026 and also serves as a test for larger, international cases in the future. We've also kept up the pressure against unlawful AI systems. *noyb* has filed its second complaint against OpenAI and has sent a cease-and-desist letter to Meta over AI training. While many details are still unclear, we see collective redress as the primary new approach to enforcement and intend to expand in this area.

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 political 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, resulting in

more DPAs becoming politicised instead of acting as independent and neutral regulators.

This fundamentally undermines the GDPR's enforcement structure, which relies primarily on DPAs as "watchdogs", rather than agencies that are primarily tasked with enabling businesses despite clear laws. In theory, **courts** should exercise oversight of DPAs. In reality, however, many courts are happy if they don't have to deal with facts around digital matters and the GDPR, and employ increasingly aggressive arguments to reject cases. While these developments are often understandable on a personal level, they increasingly create the perception that the European regulatory framework is failing and does not deliver.

In addition, the EU Commission's plans for the **Digital Omnibus** required us to increasingly share our litigation experience with policy makers and stakeholders on the European level. As the only non-profit organisation working exclusively on the GDPR for years, *noyb* had to take a more active role in the policy space. This has limited our resources for other matters, but seems to have been crucial for our mission and, so far, rather impactful.

Officially, this legislative package should have only included small, technical changes to several laws to

"simplify" EU law. In reality, the EU Commission has secretly set in motion a potentially massive reform of the GDPR that would wreck core principles, including the core definition of what constitutes personal data. Unfortunately, the quality of some parts of the legislative proposal is so poor that it would probably make the law even more complex rather than "simpler". The **lack of legal quality and consistency** is a wider trend in EU digital lawmaking, which is extremely worrying. The fact that the European Commission has – largely – moved from supporting the GDPR and baseline regulation in the tech sector to favouring deregulation is equally alarming for the digital rights sector. However, given that most elements of the GDPR are based on **Article 8 of the Charter of Fundamental Rights**, we remain confident that the current legal protections enjoyed in Europe in this area are here to stay – even if this means that *noyb* may have to engage in more **litigation to annul non-compliant EU secondary law** in the future.

We also continued to invest time and effort in expanding our data protection knowledge database **GDPRhub.** By the end of 2025, it already contained more than **4,600 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 2026 with new formats, 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 41 press releases, published hundreds of social media posts on seven different platforms and continue to be a dominant and well-received voice in the public discourse on privacy and data protection. In the future, we also aim to take a more proactive role in shaping the narrative around the GDPR. So far, this has been dominated by numerous misleading industry narratives, which have unfortunately had an increasing influence on public, political and legal debate.

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.

None of our work would have been possible without our **5,400 Supporting Members**, institutional members and every individual person who has donated to *noyb*. We deeply appreciate this support, which allows us to stay uniquely independent and to continuously work on lengthy legal procedures. We can thereby stay a stable force, especially in times of uncertainty. Thanks to your generosity and commitment, we are able to continue our work and have the meaningful impact on digital rights that *noyb* has become known for.

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

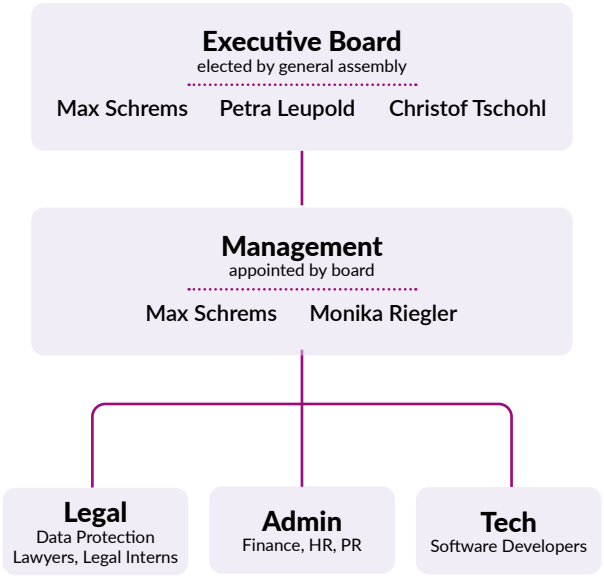
2 About *noyb*

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
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.

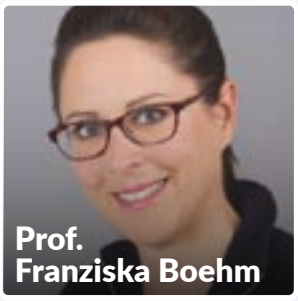
Christof Tschohl
HONORARY BOARD MEMBER

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

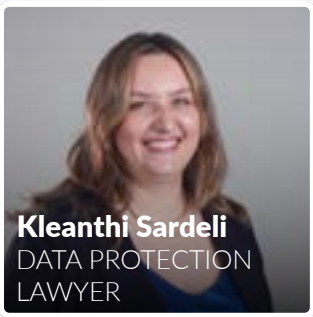
noyb's general assembly consists of four institutional members and - including our Executive Board - 17 individuals with a strong academic or legal background in the field of data protection and the GDPR in particular.

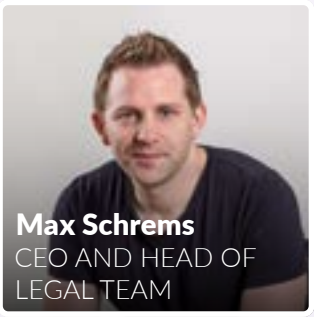


*as of Dec 2025

2.2.1.4 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.



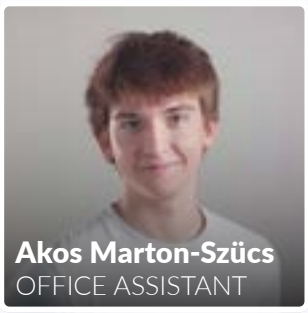


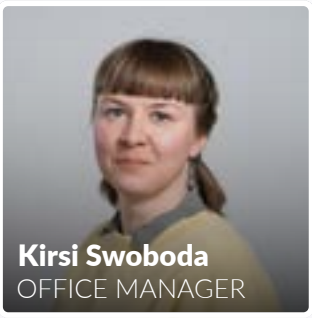
2.2.1.3 Legal Traineeships

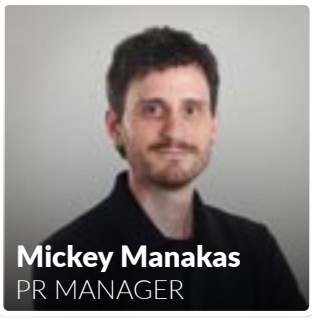
Since October 2018, *noyb* has been offering **legal traineeships** for university graduates with a strong interest in privacy law. Our trainees gain experience in legal research, factual investigation, and drafting privacy complaints. They also work on *noyb's* publicly available database, GDPRhub, and *noyb's* weekly newsletter, GDPRtoday. In 2025, **11 trainees** from **seven different countries** joined *noyb* for a period of three to six months.

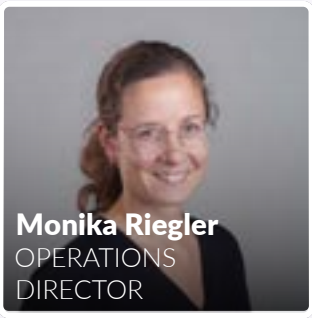
**as of Dec 2025*

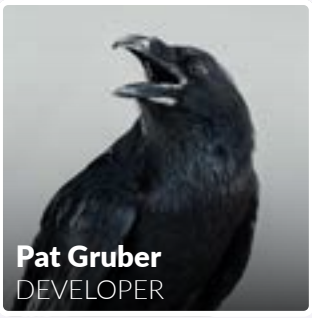
2.2.1.5 Staff — Office & Tech Team

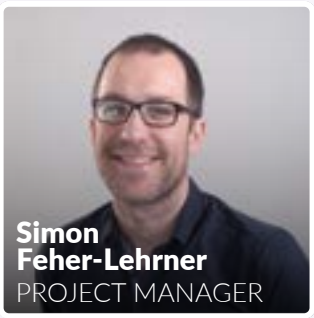


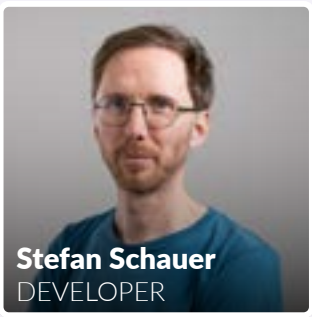












*as of Dec 2025

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 disputed. By developing complex cases targeting these 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 DPAs 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 a violation of their right to data protection.

noyb has in the past years prepared the organisational and technical means to bring collective redress actions. In 2025, *noyb* has started preparations for a potential first project.

2.3.1 Complaints

Complaints are filed with a national DPAs. 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).

Some cases have a cross-border aspect, for example if the affected user and the company involved are not located in the same country. Under the GDPR, different DPAs often have to cooperate to reach a decision in these cases.

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 national courts through proceedings that are Member State specific.

2.3.2 Lawsuits

There are two types of lawsuits. 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. Another type of lawsuit is the appeal of a complaint. This type of legal action is directed against the authority's decision. The national court then issues a decision, which can usually be appealed to a higher court. National courts (both first and second instance) have competence to refer certain questions to the CJEU, which must then 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.

3 Our Projects in 2025

In total, we have filed 21 new complaints in various jurisdictions, started preparations for our first potential collective redress case and published several reports on current legal questions in the context of data protection. Among the most significant projects is *noyb*'s preparatory steps toward a first collective redress case against the Austrian credit agency CRIF. We also filed a series of complaints against Chinese tech companies, such as TikTok and AliExpress, among other things because of unlawful data transfers to China. We've also kept up the pressure against unlawful (use of) AI systems and filed cases against Bumble and Whitebridge AI for the violation data subject rights. In 2025, *noyb* has filed its second complaint against OpenAI and sent a cease-and-desist letter to Meta over AI training.

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 Enforcement Actions

3.1.1 Preparations for a first potential collective redress project

Since 2024, *noyb* is an approved Qualified Entity in Austria and Ireland, which enables us to bring injunctions and redress measures, such as class action lawsuits. The EU system is meant to remove financial incentives for plaintiffs and only allows non-profits, such as *noyb*, to bring cases. In 2025, we started preparations for a first potential case.

3.1.1.1 Over 40,000 CRIF queries: Klarna, banks and telecoms entangled in CRIF network

Background. The credit agency CRIF collects personal data from millions of people in Austria and assesses their creditworthiness with a score. If this score is too low, those affected may find themselves unable to sign contracts with many companies, such as mobile phone providers, electricity providers, and banks. For most people, this score is based on just a few pieces of information, such as address, age and gender. These data processing activities occur without users' awareness and may not comply with the GDPR.

Call for data donations and scientific analysis. In order to test the scientific reliability of the CRIF score, *noyb* (in June 2025) has requested people living in Austria for data donations. With the participants' consent, we've obtained a copy of their data from CRIF. This enables us to compare the score with the individual's actual income situation and with the data of other participants, thereby allowing us to assess whether the CRIF score is statistically accurate. More than 2,400 affected individuals donated their data for this purpose.

noyb is currently working with a professor of financial mathematics to compare the more than 28,000 scores with the actual financial data of those affected to find out whether the CRIF scores are statistically reliable. Results are expected in the first half of 2026.

However, in September 2025, we were already able to publish a first evaluation of the data received by the participants. It shows that many well-known Austrian companies, such as Erste Bank, Verbund and Drei, evaluate their customers using CRIF data. Some companies, such as T-Mobile, the online retailer Otto, and the insurance company Allianz, also seem to provide their customer data to CRIF. The initial evaluation of over 40,000 queries with more than 28,000 scores transmitted also shows that men are rated significantly

worse than women. Also, people in cities receive a lower score than people on the countryside.

Next steps. Once the full statistical analysis of the participants' data is concluded, *noyb* will assess whether we will file a lawsuit against CRIF in our capacity as a "Qualified Entity". If personal data has been processed unlawfully, those affected could well be entitled to relevant claims for damages.

3.1.2 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* has kept 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.

3.1.2.1 Bumble's AI icebreakers are mainly breaking EU law

Background. In December 2023, the dating platform Bumble introduced so-called AI Icebreakers to the "Bumble for Friends" section of the app. Powered by OpenAI's ChatGPT, the feature is designed to help you start a conversation by providing an AI-generated message. In order to do this, your personal profile information is fed into the AI system without Bumble ever obtaining your consent. Although the company repeatedly shows you a banner designed to nudge you into clicking "Okay", which suggests that it relies on user consent, it actually claims to have a so-called "legitimate interest" to use data.

Complaint filed. In June 2025, *noyb* has therefore filed a complaint with the Austrian data protection authority (DSB). Bumble has violated its transparency obligations under Article 5(1)(a) GDPR by failing to provide information about the processing in relation to the Icebreaker feature and by confusing users with a "fake" consent banner. Furthermore, the company lacks a legal basis under Article 6(1), as it cannot legally claim to base its processing on legitimate interest and has never sought consent. This is further illustrated by the fact that the complainant's profile includes sensitive data such as sexual orientation, which can only be processed with explicit consent (Article 9). Last but not least, Bumble failed to adequately respond to the complainant's access request (Article 15).

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

3.1.2.2 AI hallucinations: ChatGPT created a fake child murderer

Background. OpenAI's highly popular chatbot, ChatGPT, regularly gives false information about people without offering any way to correct it. In many cases, these so-called "hallucinations" can seriously damage a person's reputation: In the past, ChatGPT falsely accused people of corruption, child abuse – or even murder. The latter was the case with the Norwegian user Arve Hjalmar Holmen. When he tried to find out if ChatGPT had any information about him, he was confronted with a made-up horror story: ChatGPT presented the complainant as a convicted criminal who murdered two of his children and attempted to murder his third son.

To make matters worse, the fake story included real elements of his personal life. Among them were the actual number and the gender of his children and the name of his home town. Furthermore, ChatGPT also declared that the user was sentenced to 21 years in

prison. According to Article 5(1)(d), companies have to make sure that the personal data they process about individuals is accurate.

Unfortunately, it seems that OpenAI is not capable to rectify false information in ChatGPT. *noyb* had already filed its first complaint in relation to false information in April 2024. Back then, we requested to rectify or erase the incorrect date of birth of a public figure. OpenAI argued it couldn't correct data. Instead, it can only "block" data on certain prompts, but the false information still remains in the system.

Complaint filed. On 20 March 2025, *noyb* has therefore filed a complaint with the Norwegian Datatilsynet. By knowingly allowing its AI model to create defamatory outputs about users, OpenAI violates the principle of data accuracy under Article 5(1)(d) GDPR. *noyb* is asking the Datatilsynet to order OpenAI to delete the defamatory output and fine-tune its model to eliminate inaccurate results.

Current state of the case. The complaint is still pending. Since the filing, the case has been forwarded to the Irish Data Protection Commission, which is the lead authority for OpenAI.

3.1.2.3 Ongoing project against Meta AI

In May 2025, Meta – for the second time – announced that it will start to use the personal data of Europeans for AI training. Instead of asking consumers for opt-in consent, Meta relies on an alleged 'legitimate interest' to take people's data.

noyb had already filed a series of complaints against these plans in 2024, which had prompted the Irish DPA to temporarily halt the plans. Although the legality of the plans has still not been clarified by the authorities, Meta is pressing ahead and ignoring the fundamental right to data protection of all affected Europeans.

To use personal data, companies must comply with one of six legal bases according to Article 6(1) GDPR. One of them is opt-in consent, which means that users can choose to provide a "freely given, specific, informed and unambiguous" "Yes" to the processing of their data – or to say no. However, companies can also claim a so-called 'legitimate interest' to process personal data. A thief, for example, won't consent to a CCTV camera filming him – but a bank may still have a 'legitimate interest' in having CCTV cameras for security reasons. Instead of allowing users to choose between saying "Yes" or "No", Meta is claiming that is has such a 'legitimate interest' to take their data for AI training. This leaves users with only the right to object (opt-out) under Article 21 GDPR. But Meta is even limiting this (statutory) right by saying that it only applies if people opt-out before the training has started.

Meta will likely also be unable to comply with other GDPR rights (like the right to be forgotten, the right to have incorrect data rectified or to give users access to their data in an AI system). Furthermore, Meta provides AI models (such as Llama) as open-source software for anyone to download and use. This means that Meta can hardly call back or update a model once it is published.

noyb has therefore sent a formal settlement proposal in the form of a so-called cease-and-desist letter to Meta. Other consumer groups have also taken action.

Study commissioned. A key argument in favour of such a 'legitimate interest' is the reasonable expectations of users. This begs the question: do people want this to happen? To find out more, *noyb* has commissioned the Gallup Institute to conduct a study among 1,000 Meta users in Germany. The results are clear: While almost 75% of users heard of Meta's plans, only 7% actually want their data to be used for AI training. This also means that at least 68 million people never heard about the change.

Next steps. *noyb* is currently assessing whether to bring an injunction a redress action (similar to a US class action) to recoup such damages for large user groups. *noyb* or any other Qualified Entity (see current list of the EU) can file such an action if Meta does not change its course. If the non-material damage were only € 500 per user, it could amount to around €200 billion for the roughly 400 million monthly active Meta users in Europe.

3.1.3 First complaints against Chinese tech companies

3.1.3.1 TikTok, AliExpress, SHEIN & Co send Europeans' data to China

Background. This year, we also took action against privacy violations by large Chinese tech companies. We started on 17 January 2025 by filing GDPR complaints against TikTok, AliExpress, SHEIN, Temu, WeChat and Xiaomi for unlawful data transfers to China. While four of them openly admit to sending Europeans' personal data to China, the other two say that they transfer data to undisclosed "third countries". As none of the companies responded adequately to the complainants' access requests, we have to assume that this includes China.

In principle, companies are not allowed to transfer Europeans' data outside of the EU. If, for whatever reason, they still need to do so, companies can rely on a number of legal bases. Among other things, this includes "Standard Contractual Clauses" (SCCs). For countries like China, companies usually rely on such SCCs, which are a contract in which the recipient pledges to follow EU protection standards. If companies outsource data processing, they must meet strict requirements to ensure the same level of protection of users' personal data as in the EU.

For this to be allowed, companies must conduct an impact assessment to verify that Europeans' data is secure in the destination country and that the SCCs are not conflicting with national laws that require access to data. Given that China is an authoritarian surveillance state, there is no adequacy decision and no company can provide such a guarantee as Chinese data protection laws do not limit the access by authorities in any way.

Complaints filed. *noyb* has therefore filed 6 complaints in 5 European countries and requests the data protection authorities to immediately order the suspension of data transfers to China under Article 58(2)(j) as the country does not provide an essentially equivalent level of data protection under Articles 44 and 46 GDPR. *noyb* also requests the companies to bring their processing into compliance with the GDPR. Last but not least, *noyb* asks the DPAs to impose an administrative fine to prevent similar violations in the future.

Current state of the case. All six complaints are currently pending before the national data protection authorities.

Follow-up complaints. On 17 July 2025, we've then followed up with complaints against AliExpress, TikTok and WeChat. All three tech companies have failed to comply with access requests under Article 15 GDPR. This makes it impossible for European users to exercise their fundamental right to privacy, to find out how their personal data is being processed – and if the companies actually comply with other GDPR provisions, for example regarding data transfers.

The access requests in question were originally filed in preparation for the original series of complaints. however, both TikTok and AliExpress haven't given the data subjects access to all of their data as required under Article 15 GDPR. TikTok only provided part of the complainant's data in an unstructured form that was impossible to understand. AliExpress provided a broken

file that could be opened only once. WeChat, on the other hand, just completely ignored the complainant's request.

Current state of the cases. All three complaints are currently pending with the data protection authorities.

3.1.3.2 TikTok unlawfully tracks people's online behaviour

TikTok not only tracks its users while they are using the TikTok app itself, but it is increasingly integrated with many other websites and apps.

A user found out about this unlawful tracking practice through an access request – which showed that e.g. his usage of Grindr was sent to TikTok, likely via the Israeli tracking company AppsFlyer - which allows TikTok to draw conclusions about his sexual orientation and sex life. This data is specially protected data under Article 9 GDPR, which can only be processed in exceptional cases. TikTok initially even withheld this information from the user, which violates Article 15 GDPR. Only after repeated inquiries, TikTok revealed that it knows which apps he used, what he did within these apps (for example adding a product to the shopping cart) - and that this data also included information about his usage of the gay dating app Grindr.

TikTok was only able to receive this information with the help of the Israeli data company AppsFlyer and Grindr itself. AppsFlyer most likely functions as a kind of intermediary, which receives the sensitive data about the complainant from Grindr and then passed it on to TikTok. Neither AppsFlyer nor Grindr have a valid legal basis under Article 6(1) GDPR to share the complainant's personal data with third parties such as TikTok. And they most certainly don't have any valid reason to share his sensitive data under Article 9(1) GDPR. At no point in time did the complainant consent to the sharing of his data.

Complaints filed. On 17 December 2025. *noyb* has therefore filed two complaints with the Austrian data protection authority (DSB). The first complaint is against TikTok and revolves around the incomplete reply to the complainant's access request. The second complaint is against TikTok, AppsFlyer and Grindr and deals with the undefined processing of off-TikTok data, the lack of a valid legal basis for the data sharing and processing and the violation of Article 9(1) GDPR. We request TikTok to provide the complainant with the missing information and all three companies to stop the unlawful processing of his personal data.

3.1.4 The unlawful use of Europeans' biometric data

3.1.4.1 Criminal complaint against facial recognition company Clearview AI

Clearview AI is a US company that scrapes the internet and adds all of the faces it can find in photos and videos to its database. It claims to have collected more than 60 billion photos. This allows customers of Clearview AI to identify people by uploading a photo and obtaining other pictures of the same person, including links, the name of a subpage of a website and other meta data. The company originally tried to operate largely under the radar but the New York Times revealed its practices in 2020. While Clearview AI primarily promotes its facial recognition software as a tool for law enforcement, it was also used by companies such as Walmart or Bank of America.

EU data protection authorities have already repeatedly held that Clearview AI, which processed the data of millions of Europeans, clearly violated the GDPR. The French, the Greek, the Italian and the Dutch authority imposed fines of roughly 100 million euros on Clearview for its intrusive practices. The Austrian data protection authority considered that Clearview AI has acted illegally. Several bans were issued. These decisions were not challenged by the US company.

Instead, Clearview AI is ignoring the EU authorities. Only in the UK did the company appeal the decision and fine imposed by the British ICO, with a final court decision yet to be issued. EU data protection authorities did not come up with a way to enforce its fines and bans against the US company, allowing Clearview AI to effectively dodge the law.

Criminal complaint filed. However, EU law is not limited to administrative fines under the GDPR. Article 84 GDPR also allows EU Member States to foresee criminal sanctions for GDPR breaches.

Austria has implemented such a criminal provision for certain GDPR violations in § 63 of its national Data Protection Act. In contrast to GDPR violations, criminal violations also allow actions to be taken against managers and to use the full range of criminal procedures, including EU-wide actions. For that reason, *noyb* now filed a criminal complaint with the public prosecutors in Austria. If successful, Clearview AI and its executives could face jail time and be held personally liable, in particular if traveling to Europe.

3.1.5 noyb's first complaint against a video game company

3.1.5.1 Ubisoft unlawfully collects data about your gaming habits

Background. The video game publisher Ubisoft (known for popular games like Assassins Creed, Far Cry, and Prince of Persia) forces its customers to connect to the internet every time they launch a single player game, even if the game doesn't have any online features. This allows Ubisoft to collect people's gaming behaviour. Among other things, the company collects data about when you start a game, for how long you play it and when you close it.

Complaint filed. However, the complainant had never consented to this processing. *noyb* has therefore filed a GDPR complaint with the Austrian DPA (DSB). We request the DSB to declare that Ubisoft infringed Article 6(1) GDPR with its processing of personal data without a valid legal basis. In addition, we request that Ubisoft deletes all personal information by the complainant that has been processed without a valid legal basis – and that the company ceases further unlawful processing.

Current state of the case. The complaint against Ubisoft is currently still pending with the French data protection authority.

3.1.6 Data Subject Rights

3.1.6.1 Whitebridge.ai: your personal data is for sale to you and anyone

Background. Lithuania-based Whitebridge AI sells "reputation reports" on everyone with an online presence. These reports compile large amounts of scraped personal information about unsuspecting people, which is then sold to anyone willing to pay for it. Some data is not factual, but AI generated and includes suggested conversation topics, a list of alleged personality traits and a background check to see if the person has shared adult, political, or religious content. Despite the legal right of free access to one's own data, Whitebridge.ai sells these "reports" to the affected people and denies answering access requests.

In its privacy notice, Whitebridge claims that its processing of personal data is legal and in line with its "freedom to conduct a business". By doing so, Whitebridge disregards that any business must be exercised with respect to the law, including the GDPR. Furthermore, Whitebridge AI doesn't have a legal basis to process all this personal data in the first place. Instead, the company claims to only processes data from "publicly available sources". In reality, most of this data is taken from social network pages that are not indexed or found on search engines. This has already been made clear by CJEU case law, which confirmed in C-252/21 that entering information on a social network does not constitute making it "manifestly public", which is the threshold under Article 9 GDPR.

Complaint filed. On 29 September *noyb* has therefore filed a complaint with the data protection authority of Lithuania. Whitebridge AI has violated several GDPR provisions, including Article 5, 9, 12 and 16 GDPR. We request Whitebridge AI to comply with the complainants' right of access and to rectify the false data in the reports on them. We also request the company to comply with its information obligations, to stop all illegal processing and to notify the complainants of the outcome of a rectification process. Last but not least, we suggest that the authority impose a fine to prevent similar violations in the future.

Current state of the case. The Lithuanian DPA has informed us that, further to our complaint, they considered that the issues could affect a large number of data subjects. Therefore, the DPA initiated its own investigation and cross-border proceedings. According to the Lithuanian Data Protection Act, complaints that coincide with an inspection shall not be examined. Consequently, the DPA discontinued the examination of the complaint. The DPA specified that they will inform us of the outcome of the inspection, after which we would also be able to appeal it.

3.1.6.2 WetterOnline sees "disproportionate effort" in complying with the GDPR

Background. The highly popular smartphone app WetterOnline shares the personal data of its users with hundreds of third-party companies for advertising purposes. In early 2025, this included highly precise location data which can be used to derive a user's place of residence and workplace or even more crucial information such as a visit to a military base. This data has ended up on marketplaces where it's offered for sale. Only the users themselves don't receive their data. WetterOnline refuses to provide information about processed data, claiming that complying with the GDPR's right of access would be too much effort.

Complaint filed. *noyb* has therefore filed a complaint with the data protection authority of North Rhine-Westphalia. *noyb* asks WetterOnline to fully comply with the complainant's access request and to provide both a copy of the personal data processed and information about the recipients of that data. In order to prevent similar violations in the future, *noyb* has also proposed that the competent authority impose an administrative penalty.

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

3.2 Other actions

3.2.1 Budget cuts paralyse Austrian DPA: NGO complaint to the EU Commission

Background. In September 2025, the Austrian Data Protection Authority (DSB) announced a significant restriction on its activities. The reason for this move is significant budget cuts despite an increasing workload due to a constantly growing range of tasks. However, the DSB is already underfunded compared to authorities in other EU countries. Germany, for example, spends about twice as much per capita on its data protection authorities as Austria.

According to Article 52(4) of the GDPR, Austria is obliged to provide sufficient funding for the DSB. This obligation under EU law is clearly being violated.

Complaint filed. In light of this development, *noyb* and the digital rights organisation epicenter.works have filed a complaint with the European Commission. The EU Commission then has the option of initiating infringement proceedings against Austria.

Current state of the case. The complaint still lies with the European Commission.

3.2.2 noyb takes Swedish tax authority to court for selling people's personal data

Background. In most countries, the government knows when you were born, your social security number, where you live, how much you earn and how much your house is worth. In Sweden, the tax authority doesn't just use this information for administrative purposes – but sells it to data brokers who publish it online. Earlier this year, a Swedish data subject asked the country's tax authority to stop selling his data.

The country's Supreme Court has recently ruled that freedom of information and privacy rights must be balanced and data must be marked as confidential, if the recipient is likely to process it in conflict with the GDPR. The tax authority rejected the request, claiming it simply follows the Swedish constitutional principle of transparency rather than the ruling by the Supreme Court.

Appeal filed. *noyb* has therefore filed an appeal with the Stockholm Administrative Court, requesting the tax authority to restrict the sharing of the data subject's personal information with third parties. The Supreme Court's decision makes it clear that the sharing of all this data with data brokers should be prohibited.

Selling the personal data of millions of Swedes to anyone who's interested deprives people of their fundamental right to privacy. On top of that, the GDPR's purpose limitation principle states that "personal data shall be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes". Data brokers selling the data online clearly don't comply with these rules.

Current state of the case. The Stockholm Administrative Court ruled in favour of the tax authority. *noyb* has therefore filed an appeal with the Administrative Court of Appeals, where the case is still pending.

3.2.3 Swedbank refuses transparency in automatic interest calculation

If a Bank's interest rate is set automatically and without any human intervention, even the smallest inaccuracies can cost consumers thousands of additional euros in the long run. While EU law allows the use of such an automatic system in certain circumstances, companies must follow strict rules to protect people's fundamental right to privacy. Banks, for example, would need to provide their customers with "meaningful information about the logic involved" in calculating their personal interest rate. Contrary to EU law, Swedbank rejected a Swedish citizen's access request by claiming that the calculation was a "trade secret".

According to both Swedish and EU law, a piece of information can only be a trade secret if its disclosure is likely to give competitors an advantage. But if the information is publicly available, the competitors already know. This is the case for interest rates: Transparency in mortgage lending is regulated via the EU's Mortgage Credit Directive, which literally includes the equation for the calculation of mortgage rates. In addition, the Swedish Consumer Credit Law, in a direct reference to the EU's directive, states that people are entitled to know how their interest rate was calculated, if the loan is based on a reference rate (such as the Swedish central bank's (Riksbank) policy rate) and what the bank adds on top of that rate. This is supposed to enable consumers to make an informed choice about where to lend money and to potentially correct false or incomplete data that leads to higher interest rates.

Complaint filed. *noyb* has therefore filed a complaint with the Swedish data protection authority (IMY) and requested a full investigation of Swedbank's decision to reject the data subject's access request. In order to ensure that the complainant enjoys effective protection of his rights, *noyb* subsequently proposes that the IMY orders Swedbank to provide the data subject with full access to the logic used for the calculation of his mortgage rate. In addition, Swedbank should establish procedures to adequately respond to access requests in the future.

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

3.3 Policy work

3.3.1 Digital Omnibus

Background. In November 2025, the European Commission published its proposal for the so-called Digital Omnibus, subsequently sparking significant criticism and opposition from data privacy experts and parts of the European Parliament. The reason is that, contrary to the Commission's official communications – and its initially very narrow public consultation on the topic –, the proposed legislative package contains significant changes to the GDPR. If successful, this could have a significant impact on people's fundamental right to privacy.

Among other things, the Commission proposes to narrow the definition of personal data by introducing a subjective approach. Instead of having an objective definition of personal data (e.g. data that is linked to a directly or indirectly identifiable person), a subjective definition would mean that if a specific company claims that it cannot (yet) or does not aim to (currently) identify a person, the GDPR ceases to apply. In practice, this would result in many companies effectively being exempt from the GDPR. This would apply, for example, to many data brokers and the advertising industry, which handle large amounts of personal data.

Also, the Commission wants to allow AI companies to use personal data for the training and operation of their AI systems. Specifically, the proposal suggests to enable these companies to rely on an alleged "legitimate interest", which outweighs people's fundamental right to data protection. This would create a situation, in which AI technology is given a privileged position above others. In practice, this would mean that an otherwise illegal processing could suddenly become legal, simply because it is done using AI.

Thirdly, the Commission wants to restrict the right of access under the GDPR to "data protection purposes" only. This would allow companies to label access requests as "abusive" if they serve a purpose other than gaining access in itself. Conversely, this means that if an employee uses an access request in a labour dispute, for example over unpaid hours – for example, to obtain a record of the hours they have worked – the employer could reject it as "abusive". The same would be true for journalists or researchers.

Fourth, the Commission has proposed new, very broad definition of "scientific research", which could be abused by profit-oriented private actors – who then would be exempt from the GDPR obligations regarding purpose limitation and the right to information. In practice, this change could enable companies to claim that they are conducting scientific research, when they're actually using personal data to train their AI systems with even fewer restrictions.

What we did. When we found out about the proposal, *noyb* took immediate action. Among other things, we teamed up with 126 other civil society organisations to send two open letters to the European Commission, communicating our concerns.

We also prepared a deep dive video analysis of the proposal and published a 70-page report including suggestions for lawmakers.

Speaking of which: We of course immediately started reaching out to lawmakers to discuss the issues with the proposal and make sure that your fundamental right to data protection remains intact. Thanks to media outreach, we also spread public awareness within the privacy community and beyond.

What's happening next. The Digital Omnibus is far from being signed into law. The European Commission's proposal is currently being discussed in the European Parliament and the Council. It is therefore up to these two institutions to prevent any changes that would undermine the foundations of the GPDR. In the meantime, *noyb* will continue to work towards the best possible outcome.

3.3.2 GDPR Procedural Regulation

Background. Since becoming applicable in 2018, the GDPR aims to ensure that Europeans enjoy privacy rights across the EU. However, when people's rights are violated by companies based in another EU/EEA Member State, complaints are dealt with through a complex "cooperation mechanism" between the DPA in the users' Member State and the DPA in the company's Member State. This enforcement mechanism is at the core of the generally acknowledged enforcement failure of the GDPR. Complaints get lost, decisions take years and there is virtually no possibility to act against inactive DPAs. In 2023, the EU has ventured to solve this through a GDPR Procedural Regulation.

However, it quickly became clear that the European Commission's proposal actually risks undermining the GDPR's enforcement by introducing excessively long deadlines and overly complex procedures. Alarmingly, the proposal even suggested to largely remove data subjects from the procedure.

Immediate action. Naturally, *noyb* immediately took action, both through media initiatives, an explainer video, and by reaching out to lawmakers in an attempt to ensure that cross-border procedures do not become overly complicated and that data subjects do not become bystanders having no say in proceedings regarding their fundamental right to data protection. The European Parliament and Council took into consideration some of the most pressing concerns voiced by *noyb* and ensured some basic procedural rights for data subjects. Regrettably, the general trajectory of the Commission's proposal prevailed in many regards, possibly leading to more confusion and complexity rather than increased efficiency of cross-border procedures. *noyb* will monitor the application of the Procedural Regulation, which will become applicable in April 2027 and report on its impact in practice.

3.4 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 2025, we also published our Pay or Okay report, analysing the industry's arguments for the system and the actual economic impact of Pay or Okay.

3.4.1 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 2025, the number of decisions collected and summarised has grown to more than 4,600, with more than 14,000 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.

3.4.2 Analysis of DPO activities in Europe: Only 1.3 % of cases result in a fine

Background. When the General Data Protection Regulation (GDPR) came into force in 2018, it ushered in a new era of data protection in the EU. At least on paper. Consumers were given the tools to stand up for their fundamental rights, while authorities received serious investigatory powers and the ability to sanction breaches with hefty fines. However, the reality is much bleaker, a *noyb* analysis shows of DPA activity between 2018 and 2023 shows: On average, merely 1.3% of cases before DPAs result in a fine.

While some data protection authorities appear to impose far more fines than others, the figures are all in the single-digit percentage range – or even lower. Having imposed fines in 6.84% of all cases (counting both complaints and own-initiative investigations) between 2018 and 2023, the Slovakian DPA is leading the statistics. It is followed by Bulgaria (4.19%), Cyprus (3.12%), Greece (2.65%) and Croatia (2.54%). At the

other end of the spectrum, the Dutch authority has issued fines in 0.03% (!) of all cases, closely followed by France (0.10%), Poland (0.18%), Finland (0.21%), Sweden (0.25%) and of course Ireland (0.26%). The remaining countries are somewhere in between.

While these numbers are hardly surprising, they're alarming nonetheless. A *noyb* survey from 2024 among data protection professionals shows that it is precisely monetary fines that motivate companies to comply with the law. When asked about the most effective enforcement measures, 67.4% of respondents said that DPA decisions against their own company that include a fine will influence decision makers to opt for more compliance. Interestingly, 61.5% of respondents said that even fines against other organisations would influence their own company's GDPR compliance.

3.4.3 In-depth research into Pay or Okay systems in Europe

Background. So-called 'Pay or Okay' systems are on the rise in Europe. First introduced by newspapers in Austria and Germany, Meta adopted the approach for Instagram and Facebook in 2023. By now, many websites across Europe are using similar systems. Instead of giving users a genuine choice whether to accept or reject ad tracking (as required by the GDPR), 'Pay or Okay' systems request a payment if they want to refuse "consent". This leads to "consent" rates of up to 99.9%. Many news companies claim that the approach is necessary to finance quality media.

One report, one survey. In order to assess the actual preferences of affected users and to analyse the industry claim that such systems are necessary for survival, *noyb* published two reports on the topic in 2025.

Survey. Users prefer a tracking-free "third option". The results of *noyb*'s study on user preferences are clear. When asked openly, only about 2 out of 10 people agree with companies collecting and analysing their data. When they face a "pay" and a "consent" option, however, about 9 out of 10 people still choose "consent". The high consent rate seems to be caused by the lack of a reasonable alternative. In reality, most users prefer a tracking-free option. When they are given the choice between "pay", "consent" and "advertising, but no tracking", most users (7 out of 10) choose the tracking-free third option.

The survey also shows that users do not behave differently depending on whether they are on large social networks, journalistic pages or other websites. Therefore, there is no factual basis to treat these websites differently and, e.g., create different Pay or Okay guidelines for media websites than for social media.

Report. How companies make you pay for privacy. Proponents of 'Pay or Okay' largely rely on an alleged economic need to finance quality media and claim that personalised advertising is the source of revenue that will rescue struggling news media.

However, this claim is not supported by reality. *noyb*'s Pay or Okay report shows that digital advertising makes up at best 10% of the revenue of European press. Targeted advertising is even less: Only about 5% of newspaper and magazine revenue stems from the processing of personal data for advertising purposes.

Most companies argue that 'Pay or Okay' is supposed to allow some form of economic fairness. However, the cost for the Pay option is very high when compared to the advertising revenue. Academic research shows that publishers earn € 0.24 per user and month from tracking – while choosing the Pay option generates € 3.24 per user and month. The same research highlights that 'Pay or Okay' increases 'cookie banner related income' by 16.4%. Given that on average only 5% of press revenue comes from programmatic advertising, 'Pay or Okay' would only increase the overall income of the press by 0.82% on average.

This has also drawn the attention of the authorities. The European Data Protection Board (combining all the EU data protection authorities) is currently drafting guidelines on the topic, which will provide more legal clarity in this matter. The publication of the guidelines is currently expected sometime in summer 2026.

3.5 Updates on ongoing projects

3.5.1 Years of inactivity in "Pay or OK" cases: *noyb* sues German DPAs

Background. In August 2021, *noyb* filed two GDPR complaint against the 'Pay or OK' banners on the news sites faz.net and t-online.de. At the time, the complainant (and all other users) had to decide whether to allow the websites to process and distribute their personal data for ad tracking or to take out a paid subscription in order to have their privacy respected. The GDPR explicitly requires that consent must be "freely given". Nevertheless, more than 99.9% of users agree to tracking when faced with 'Pay or OK'. In the meantime, even the EU Commission has considered that this approach is illegal in a case against Meta.

Almost four years after the filing of the complaints, the DPAs of North Rhine-Westphalia and Hesse still haven't managed to issue a decision on the merits. Quite the opposite: In order to avoid finally deciding the case, the DPA of North-Rhine Westphalia has even issued a 12-page decision that it cannot decide yet.

Lawsuits filed. The complainant in the cases against t-online and faz.net has therefore filed two lawsuits with the Administrative Courts of Wiesbaden and Düsseldorf, respectively. If the action is successful, the authorities would have to decide and uphold the initial complaints.

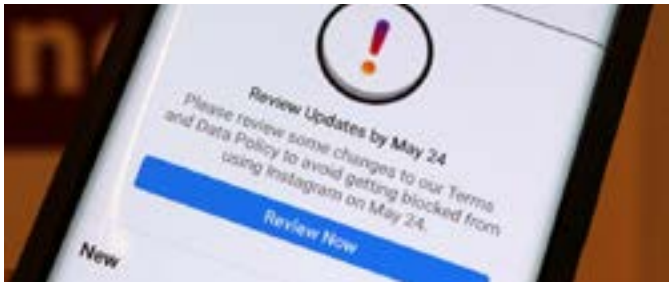
Current state of the cases. Both lawsuits are still pending with the respective Administrative Courts.

3.5.2 EU Court: Irish DPC must investigate *noyb* complaint

Background. When the GDPR came into force on 25 May 2018, *noyb* had immediately filed complaints against Google, Facebook, Instagram and WhatsApp for relying on "forced consent" to process user data.

The complaint against Facebook was quickly forwarded to the Irish Data Protection Commission (DPC). In 2021, the Irish DPC issued a draft decision and shared it with the other European data protection authorities for review. Several authorities raised objections. This led to the Irish DPC referring the case to the European Data Protection Board (EDPB), initiating the GDPR's dispute resolution procedure.

Binding decision. In December 2022, the EDPB then published its binding decision on the matter and held that Meta illegally used the personal data of users for advertising without a valid legal basis under Article 6(1) GDPR. The EDPB also decided that the DPC should have also investigated the use of sensitive data (Article 9 GDPR).



Final ruling. However, the DPC sued the EDPB before the European Courts, arguing an overreach by the EDPB. This was unsuccessful. In its ruling from 29 January 2025, the EU's General Court has dismissed the DPC's claims. The ruling is final and can't be appealed anymore.

3.5.3 Austrian Supreme Court: Meta must give users full access to their data

Background. Since 2011, the plaintiff Max Schrems has tried to get full access to his personal data, but Meta only provided him partial access. For "average" users, Meta usually only refers to a "download tool" that contains what it calls "relevant" information and otherwise refers to its generic privacy policy. However, under Article 15 GDPR, Meta must provide not only a full 1:1 copy of all personal data to any user that requests it, but also provide information as to the purposes this data was processed for and the sources and recipients of all information.

The case, brought by Max Schrems in 2014, originally lasted 11 years and hit the Austrian Supreme Court three times and the European Court of Justice two times.

Final court ruling. In December 2025, the Austrian Supreme Court then decided that Meta must disclose all personal data (each and every bit) and also provide specific information on all data, such as the source, recipient or purpose of processing, all within a 14-day deadline ending on 31.12.2025. The default deadline under the law is one month – which has lapsed already years ago. Meta's claims on alleged limitations of any full right to access (such as trade secrets and alike) were not properly argued by Meta and hence fully rejected. The final and directly enforceable ruling by the Austrian Supreme Court will therefore lead to unprecedented access by Mr Schrems to Meta's practice of processing his (and in reality, anyone else's) user data.

3.5.4 Conde Nast fined €750,000 for placing cookies without consent

Background. In December 2019, *noyb* had filed complaints against three providers of French websites, because they had implemented cookie banners that turned a clear "NO" into "fake consent". Even if a user went through the trouble of rejecting countless cookies on the eCommerce page CDiscount, the movie guide Allocine.fr and the fashion magazine Vanity Fair, these websites sent digital signals to tracking companies claiming that users had agreed to being tracked online. CDiscount sent "fake consent" signals to 431 tracking companies per user, Allocine to 565, and Vanity Fair to 375, an analysis of the data flows had shown.

Decision by the CNIL. On 27 November 2025, almost six years after these complaints had originally been filed, the French data protection authority CNIL has finally reached a decision in the case against Vanity Fair: Conde Nast, the publisher behind Vanity Fair, has failed to obtain user consent before placing cookies. In addition, the company failed to sufficiently inform its users about the purpose of supposedly "necessary" cookies. Thirdly, the implemented mechanisms for refusing and withdrawing consent was ineffective. Conde Nast must therefore pay a fine of €750.000.

3.5.5 Microsoft 365 Education may not track school children

Background. During the COVID pandemic many schools quickly shifted to cloud products and Big Tech was quick to provide "educational" products. However, Microsoft shifted all responsibility to comply with privacy laws onto schools and national authorities – that have little to no actual control over the use of student data. Local schools are usually not powerful enough to push back against Microsoft - leading to a "take it leave it" situation.

When faced with a student's access request to personal data processed by Microsoft 365 Education, this led to massive finger pointing: Microsoft simply referred the complainant to its local school. However, the school of the complainant could only provide minimal information

- as it does not have any way to access information that rests with Microsoft. No one felt able to comply with GDPR rights. The complainant, represented by *noyb*, consequently lodged a complaint against all possible players (the local school, the local board of education, the Ministry of Education and Microsoft US) with the Austrian DSB.

DSB decision. The Austrian DSB found several GDPR violations. First, it found Microsoft 365 Education used tracking cookies without consent, which was found to be illegal. Both the school and the Austrian Ministry of Education claimed during the procedure they were not aware of such tracking cookies before the complaint.

The DSB now ordered the deletion of the relevant personal data. Second, Microsoft violated the right to access under Article 15 GDPR by not providing full access to the data of the complainant. Microsoft will now have to provide such access. Microsoft will also have to explain in clear terms what it means that it uses data for its business purposes such as “business modeling” or “energy efficiency” and if it sent personal data to LinkedIn, OpenAI or the tracking company Xandr.

3.5.6 Court decides "Pay or Okay" on DerStandard.at is illegal

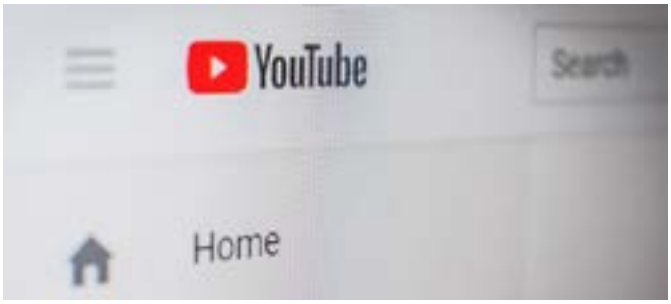
Background. DerStandard is the leading liberal newspaper in Austria and was the first website that introduced a so-called Pay or Okay approach when the GDPR came into force. Instead of giving users a genuine choice between agreeing to and rejecting online tracking by hundreds of third parties, it asked users to either consent or pay for a monthly subscription.

In a more political than legal decision from 2023, the Austrian Data Protection Authority (DSB) took the view that there was no general issue with "Pay or Okay" – ignoring the fact that there is a 99.9% consent rate. At the same time the DSB held that DerStandard's approach to "Pay or Okay" was unlawful as it only allowed a global consent or rejection – when the law requires the option to consent to specific types of processing. DerStandard appealed and argued that such a "granular" consent is not doable in a "pay or okay" system, as it e.g. required tracking and statistics to sell its advertisement in the non-paid version.

Court decision. In August 2025, the Austrian Federal Administrative Court (BVwG) confirmed the DSB’s decision that DerStandard did not obtain valid consent, rejecting the appeal by the newspaper. At the same time, it allowed an appeal to the Supreme Administrative Court (VwGH) given that the issue is novel and not decided by Supreme Courts yet. It is very likely that the Supreme Administrative Court would refer this case to the EU Court of Justice (CJEU).

Current state of the case. DerStandard now offers granular options in its consent banner. Part of the proceedings has been referred back to the data protection authority and has not yet been decided.

3.5.7 YouTube ordered to honour user’s right of access



Background. In January 2019, *noyb* filed eight complaints against a series of streaming providers such as Amazon, Apple Music, Spotify, Netflix and YouTube. 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 provide users with a copy of their personal data, as well as additional information about the processing, such as details on the sources and recipients of the data, the purpose for which the data is processed and the retention period.

The case against YouTube (and therefore against Google) was simple and should have been easy to decide. The company had only provided a fraction of the data

that it processes about the complainant and withheld information about the purpose of the processing, storage periods, data recipients and tracking cookies used.

DPA decision. In late August 2025, the Austrian data protection authority (DSB) then issued a decision siding with *noyb* – and ordering YouTube to comply with the complainant's access request in accordance with Article 15 GDPR.

3.5.8 French DPA fines Google €325 million for "Spam Emails" in Gmail

Background. More than three years ago, *noyb* had filed a complaint against Google for sending unsolicited advertising emails directly to the inboxes of Gmail users. Contrary to EU law, the company never asked the people concerned for their consent.

DPA decision. The French data protection authority CNIL has now sided with *noyb* and found that Google's implementation of spam advertising in Gmail violates its consent obligations under EU law. In addition, the authority said until October 2023, Google made it too difficult for users to refuse cookie consent when setting up their Gmail account. The CNIL has therefore imposed a fine of €325 million against Google.

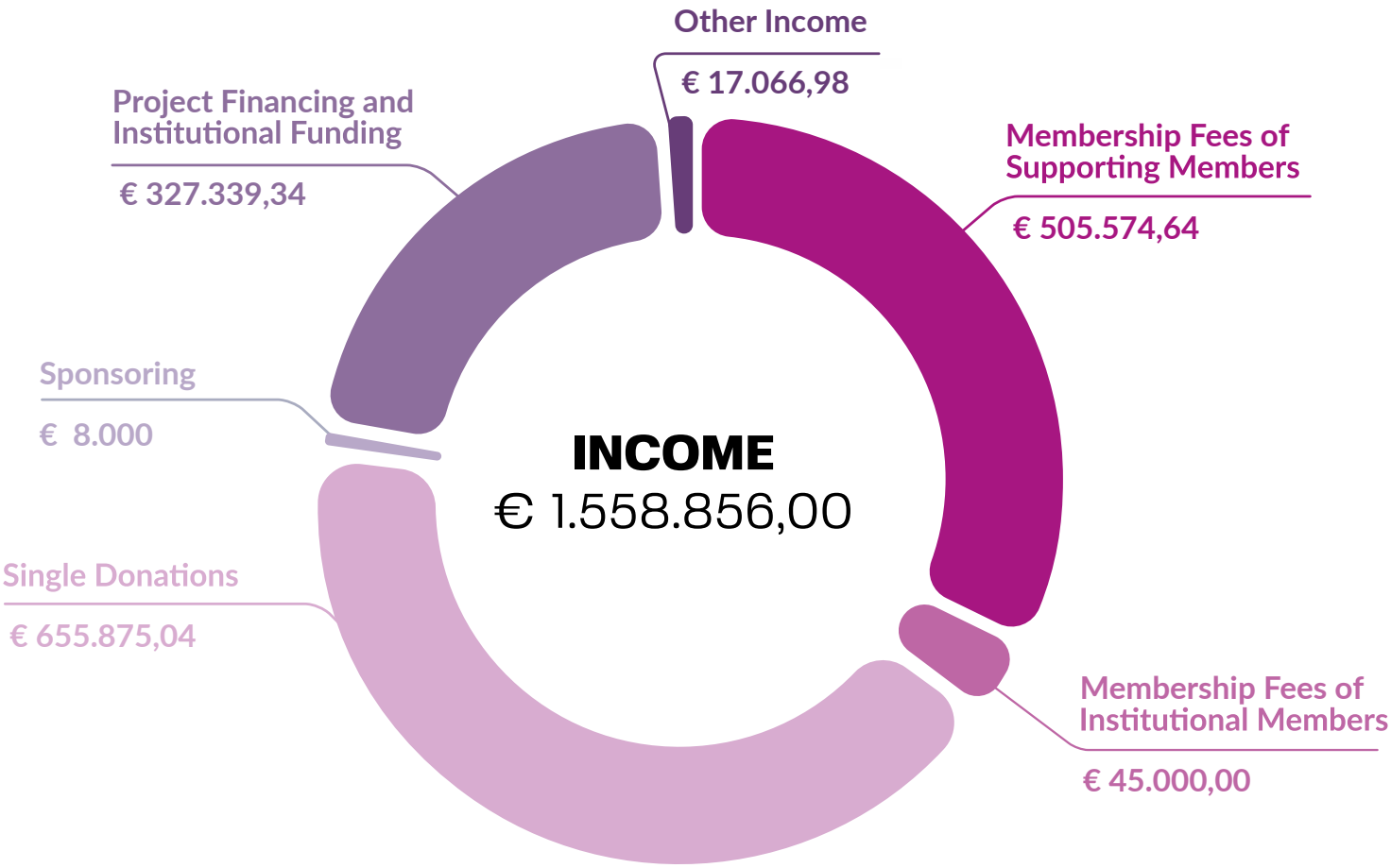
3.5.9 Austrian authority forbids unlawful credit scoring by KSV1870

Background. In August 2024, *noyb* had filed a complaint against KSV1870 and the energy provider Unsere Wasserkraft with the Austrian Data Protection Authority (DSB). The complainant, represented by *noyb*, was subjected to a fully automated credit rating by KSV1870 without being asked. This led to a – likewise fully automated – refusal of Unsere Wasserkraft to conclude a contract with the data subject. All this happened without the potential customer being informed. The GDPR makes it unambiguously clear that fully automated decisions with such far-reaching consequences are generally prohibited (with only a few exceptions).

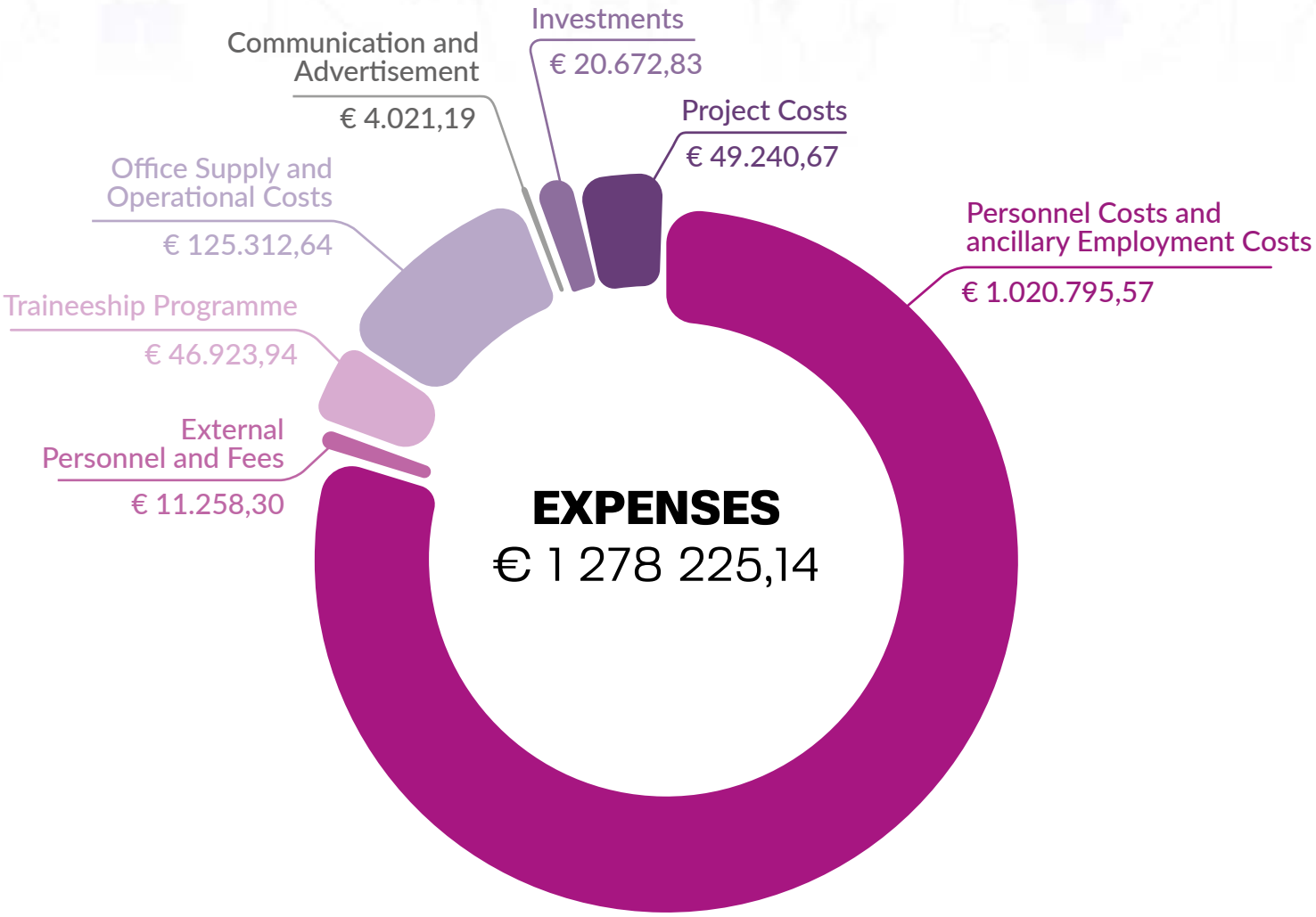
With regard to automated credit ratings by credit information agencies, the CJEU already clarified in 2023 that such a practice is unlawful. In its ruling on a case against the German credit information agency SCHUFA, the Court stated that if companies use the results of a credit assessment as a decisive factor in their decisions, this credit rating is considered a prohibited decision under Article 22 GDPR. Only if special conditions are met – such as the explicit consent of the data subject – would such a decision be permissible.

DPA decision. The DSB has now clarified that KSV1870's actions violate the prohibition of automated individual decision-making and that the credit information agency has not complied with the respective transparency obligations. It is noteworthy that the DSB has not only instructed KSV to provide a comprehensible explanation of the (unlawful) credit rating. The authority has also issued a ban on carrying out automated credit checks using the complainant's data in future without his consent. The DSB also reprimanded the approach taken by the energy provider Unsere Wasserkraft. In connection with the fully automated rejection of the complainant, the supplier violated its transparency obligations. If Unsere Wasserkraft wishes to continue assess the creditworthiness of its potential customers, it must adapt the relevant processes to bring them into compliance with applicable data protection law.

4 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



- **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

5 *noyb* in the media


Privacy firm files Ubisoft legal complaint over data collection, forced online in single-player games
EUROGAMER
Ubisoft Complaint »
Datenschutzorganisation Noyb nimmt Kreditauskunftei CRIF ins Visier
ORF.at
CRIF »
Digitaler Omnibus
„Die EU-Kommission rüttelt an den Grundpfeilern des Datenschutzes“
NETZPOLITIK.ORG
Digital Omnibus »
Sign in
The Register
LEGAL
Clearview AI faces criminal heat for ignoring EU data fines
Noyb says New York-based facial recognition
Connor Jones
The Register
Clearview AI »
PRO TECH
Google handed €325 million fine in France over Gmail ads and cookies
EURACTIV
Google fined €325 million over ads and cookies »
SPIEGEL Netzwelt
TikTok, Shein, AliExpress & Co.
Datenschützer legen Beschw
gegen chinesische Firmen ei
DER SPIEGEL
TikTok, AliExpress & WeChat »
TABLE OF CONTENTS
16.01.2025, 15.49 Uhr
EuroEFE:
Denuncian a TikTok, AliExpres
y WeChat por incumplir la
legislación europea de
privacidad
17 julio 2025
EuroEFE:
TikTok, AliExpress & WeChat »

6 *noyb* in numbers

5 400 Supporting Members

20 Team Members

11 Legal Trainees

21 **Complaints** filed in 2025

460 **Cases** pending

>50 **Cases** closed, withdrawn or lost by authorities

€ 2 billion in fines

41
Press Releases

12
Newsletters & Member Updates

>89 000
Followers on 6 media platforms

GDPR hub

4 600 Summaries on GDPRhub

>300 Country Reporters

>14 000 Subscribers to GDPRtoday

8 Country Reporter Meetings

**as of Dec 2025*

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

dialogMail eMarketing Systems

DuckDuckGo

apecdata

LamaPoll

foundata

freedom internet

LIONWARE

devowl.io

Proton Pass

Imprint:
noyb – European Center for Digital Rights

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

ZVR: 1354838270