noyb

European Center
for Digital Rights

Annual Report

2020

noyb.eu

TABLE OF CONTENTS

Preface

2020 marks **noyb**'s third year fighting for your rights. After being busy setting up our organization, developing processes and building a strong team in the past two years, 2020 was the year in which we could truly focus on our legal work and our enforcement strategy.
Although GDPR has been in place for more than two years, we still experience and struggle with teething problems that came with it: Authorities not doing their job, companies willfully "reinterpreting" the regulations or not complying with the law at all.

In 2020 we were able to fight back and show our teeth: In our long lasting case on EU-US data transfers ("Schrems II") the European Court of Justice invalidated the Privacy Shield and substantially changed how data transfers need to be handled in the future. We filed 101 complaints against controllers still forwarding data to the US in August 2020 which lead to a specific task force of the EDPB, we provided information for EU companies on how to comply with the ruling and informing users about their options to stop data transfers to the US. Furthermore, **noyb** is fighting a legal battle with the Irish Data Protection Commissioner, the responsible authority for Facebook, to enforce the judgment and stop Facebook's data transfers to the US. Representatives of **noyb** were participating in hearings and discussions on future data transfer mechanisms. We commented on a draft by the European Commission on Standard Contractual Clauses (SCCs) to have an impact on how future data transfer mechanisms will be designed. But our work was not limited to data transfer, we also filed numerous complaints to fight against infringements of the GDPR, being it violations of data subject rights or online tracking.

As for many others, 2020 was a tough year for us at **noyb**. We spent numerous months working from home and having our meetings remotely. Our international team was suddenly very limited in travels, our office was rearranged several times to make it Corona-safe: we put up partition curtains, changed our bathroom into a makeshift kitchen, ensured weekly tests for all team members and aired out the office far more often than the weather would have allowed it, in order for our team to stay safe and healthy. Being a donation-funded NGO is not an easy thing in tense economic times as we strongly depend on supporting members, institutions, public funding and donations by pro-privacy businesses. We are all the more grateful to our long-standing and also newly acquired supporters for supporting and enabling us to continue our work beyond this crisis year 2020. Thank you very much!

Back in 2018, **noyb** was merely an idea. Now, I am proud to look back on our year 2020 and see how this organization has quickly developed: In 2020 we were able to grow our team by three and at the end of 2020, 15 people from 10 different countries worked in our office in Vienna. This team has been filing more than 125 complaints. Five of our cases are currently handled in courts. **Substantial fines** have been imposed based on our complaints. Our work was covered in more than **275 newspaper articles**, we gave numerous interviews for newspapers, television and radio stations and participated in webinars.
But we are not planning to stand still in the upcoming year: **noyb** is constantly engaging in GDPR enforcement, challenging decisions of data protection authorities and developing new cases on all relevant articles of GDPR. In 2021 one focus will be on collective actions: In September 2020, **noyb** was approved as **a "qualified entity" in Belgium** and can therefore file representative actions and claim damages on behalf of users in Belgium. In 2021 we will prepare for the implementation of the collective redress directive which will enter into force in 2022 and allows us to file class actions for data protection violations.

Another key project in 2021 will be on online tracking, since most website operators are still not legally compliant when it comes to the use of cookies and other forms of online tracking. We hope to bring a number of cases that will transform how users are bothered with consent banners in the course of 2021. We also acknowledge that users still often have a hard time to exercise their rights under the GDPR. In this context, we will further develop methods for informing the public about how they can concretely access, correct or delete their data.

Thank you for your interest in **noyb** and your support!

Max Schrems, Chairman and Managing Director

About noyb

Our Mission

noyb uses best practices from consumer rights groups, privacy activists, hackers, and legal tech initiatives and merges them into a stable European enforcement platform. Together with the enforcement possibilities under the EU data protection regulation (GDPR) which is in place since May 2018, **noyb** can submit privacy cases on behalf of affected users.

Additionally, **noyb** follows the idea of targeted and strategic litigation in order to strengthen the right to privacy. We also make use of PR and media initiatives to support the right to privacy without having to go to court.

Last but not least, **noyb** is designed to join forces with other organizations, resources and structures to maximize the impact of GDPR, while avoiding parallel structures.

More information can be found in our **concept**.

Who we are

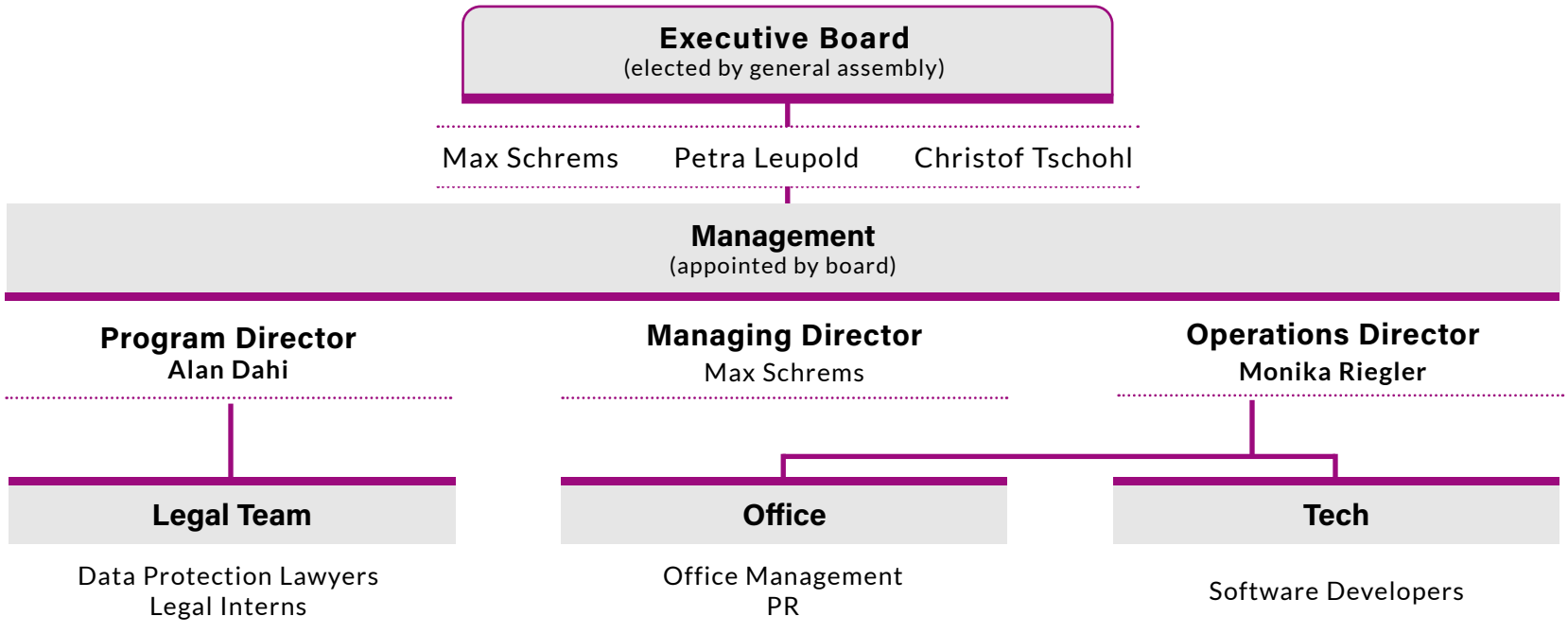
Organigram & Governance

The General Assembly meets once every two years and appoints the executive board. It consists of distinguished individual members that are deeply commitment to privacy, the GDPR, and the enforcement of fundamental rights and representatives of our institutional members, such as the City of Vienna, Austrian Chamber of Labor and others.

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

The Executive Board can appoint one or more Directors that manage the daily business within the office and who may represent **noyb** for any matter.

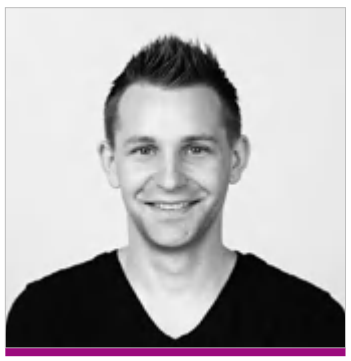
In addition to Max Schrems, who acts as a pro-bono Managing Director of **noyb** since its founding, Alan Dahi was appointed as Program Director and is leading the Legal Team. Monika Riegler is responsible for all administrative affairs of **noyb**.



EXECUTIVE BOARD

MAG. MAX SCHREMS

HONORARY CHAIRMAN AND MANAGING DIRECTOR



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

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

DR. PETRA LEUPOLD, LL.M.

HONORARY BOARD MEMBER

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

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

DR. CHRISTOF TSCHOHL

HONORARY BOARD MEMBER

Christof Tschohl successfully brought down the Austrian data retention legislation and is the chairman of epicenter.works, which is dedicated to defending our rights and freedom on the Internet. Furthermore, he is the scientific director of Research Institute – Digital Human Rights Center. He holds a Doctorate of 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."*

STAFF

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

Legal Team

ALAN DAHI

PROGRAM DIRECTOR

"A resilient society needs strong digital rights. We help ensure these."

ALA KRINICKYTE

*"Data subjects have to acknowledge their rights and be able to successfully enforce them. I want to help **noyb** embed a new privacy and data protection culture in the digital world."*

MARCO BLOCHER

*"In an ever changing digital world, the right to privacy is the backbone of the individual's freedom. I am excited to be part of **noyb**'s journey to help this freedom unfold"*

STEFANO ROSETTI

*"My main interests are digital rights and litigation. **noyb** gives me a fantastic opportunity to practice both from a unique point of view"*

ROMAIN ROBERT

*"I am so excited to have joined **noyb.** Digital rights and data protection should become a reality."*

Traineeships

Since October 2018, **noyb** has been offering legal traineeships for university graduates with a strong interest in privacy law. Our trainees obtain experience in legal research, factual investigations, and drafting complaints.

Furthermore, they work on **noyb**'s publicly available database GDPRhub and **noyb**'s weekly newsletter GDPRtoday. In 2020 ten trainees from eight different countries joined **noyb** for a duration of three to nine months.

STAFF

Office & Tech Team

MONIKA RIEGLER

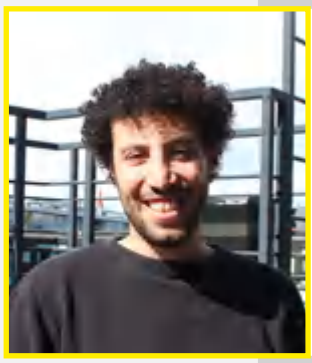
OPERATIONS MANAGER

*"I am more than happy to be part of **noyb** from the very beginning and to help building a strong organization to enforce our right to privacy."*

PHOEBE BAUMANN

PR MANAGER

*"Digital rights and data protection means fighting for the people rather than for the corporations illegitimately profiting through our data. **noyb** puts the control over our own identity back into our hands. And that is why I truly enjoy working here."*



ANAS ZAHED

OFFICE AID

*"Especially after the data scandal at Cambridge Analytica, I think there is a need to campaign for data protection. **noyb** is just the beginning and I'm happy to be part of it."*

HORST KAPFENBERGER

SOFTWARE DEVELOPER

„Good karma to the ones reading that far"

MUX

SOFTWARE DEVELOPER

"The internet is made of cats"

How we work

Many companies ignore Europe's strict privacy laws. They take advantage of the fact that, too often, it is too complicated and expensive for individual users to enforce their rights. In May 2018, the new General Data Protection Regulation (GDPR) came into force – heralding a new era in EU privacy protection with new enforcement mechanisms.

Article 80 of the GDPR allows NGOs, such as **noyb**, to collectively enforce digital rights.

noyb pursues strategic and effective enforcement by thoroughly analyzing and prioritizing privacy violations, identifying the legal weak spots of these cases and litigating them with the best possible strategy and the most effective method to achieve maximum impact.

noyb either files complaints against companies to the responsible data protection authority (DPA) or brings cases to courts.

Complaints

Complaints are a cost-effective way to enforce the GDPR. They are filed with a national data protection authority. An unsuccessful complaint can be appealed with the courts.

We decide whether to lodge a complaint based on the following factors:

- **High and direct impact**: A case or project should directly impact many people (a whole industry or a common practice across different sectors and across Europe).
- **High Chances of Success**: Lost cases backfire on our overall aim of promoting privacy. There may be "edgy" cases or cases that just need clarification that are worth the risk.
- **High Input/Output Ratio**: We only engage in cases or projects that have a good input/output ratio in order to maximize the use of our funds.
- **Strategic**: Strategic litigation is based on considering all elements that may affect the case or project and making informed decisions on these elements. For example, if a Data Protection Authority states that they will be focusing on a certain subject matter, it may make sense to file a complaint with that authority. Each case should have ideal timing, jurisdiction, costs, fact patterns, complainants, and controllers.
- **Narrow and Well-Defined**: Many controllers violate just about every Article of the GDPR. We pick the relevant part only.

Lawsuits

There are two types of lawsuits.

The first are lawsuits directly against a company. Such lawsuits typically cost more than complaints, but are an equally - if not more so - powerful tool than complaints. One advantage that lawsuits have over complaints is that they are not subject to a cross-border procedure, as would be the case with a complaint against a company located in a different Member State than where the data protection authority the complaint is lodged against, is.

For example, cross-border procedures will apply when a user lives in Austria but the company they are filing against is based in Ireland.

Another type of lawsuit is in the appeal process of a complaint. Such a lawsuit is against the decision of the authority. It is a parallel to how one may appeal the decision of a lower court to a higher court.

Our projects

In 2020, our main focus was on EU-US data transfers, as **noyb** supports the previously existing case of Max Schrems on Facebook's data transfer to the U.S. Not only did **noyb** file several new complaints in 2020 and also pushed forward already existing complaints, but also dissemination of GDPR related information was on our plate this year.

- Major developments are published on our website's homepage.
- An overview of ongoing projects can be found on our project page.

3.1 EU-US Data Transfers

3.1.1. Juridical Review against the DPC
3.1.2 Mass complaint on EU-US Data Transfers
3.1.3 FAQs for Controllers and Users
3.1.4 Feedback on future data transfer mechanisms

3.2 Mobile tracking

3.2.1 Complaint against Google's Android Advertising ID
3.2.2 Complaint against Apple's Identifier for Advertisers

3.3 Encryption

3.3.1 Complaint against Amazon

3.4 Data Subject Rights

3.4.1 Complaint against A1 Telekom Austria
3.4.2 Complaint against address broker AZ Direct GMBH
3.4.3 Complaint against Wizz Air
3.4.4 **noyb**'s Exercise your Rights Series

3.5 Credit Ranking Agencies

3.5.1 Complaint against credit ranking agency CRIF

3.6 Data breaches

3.6.1 Complaint against IT Solutions "C-Planet"

3.7 Dissemination

3.7.1 GDPRhub and GDPRtoday

3.8 Research

3.8.1 Report on Streaming Services
3.8.1 Report on privacy policies of video conferencing services
3.8.3 Report on SARS-CoV-2 Tracking under GDPR
3.8.4 Review of Austrian "Stopp Corona App"

3.9 Updates on past projects

3.9.1 Streaming complaints
3.9.2 Forced Consent - Google
3.9.3 Grindr

PHOTO BY ALEV TAKIL / UNSPLASH

3.1 EU-US Data Transfers

noyb is supporting the case by Max Schrems on EU-US data transfers. This second lawsuit before the Irish Courts was triggered after the "Safe Harbor" judgment in 2015 and is basically a second reference on the same case. Currently so-called "Standard Contractual Clauses" (SCCs) are used by Facebook Ireland to transfer data to US servers. Under U.S. law intelligence services such as the NSA have access to these servers. Individuals whose data have been accessed by U.S. intelligence services will not receive any information on this and do not have the possibility for judicial redress before U.S. courts. All "European" data that is stored in US "cloud" services is therefore not properly protected, as it would be foreseen under EU law. This case has been pending since 2013 and the background of this case can be found here.

3.1.1. COURT OF JUSTICE JUDGMENT ON PRIVACY SHIELD

On July 16 2020, the Court of Justice of the European Union invalidated Privacy Shield and decided that Facebook and other companies that fall under US surveillance laws cannot rely on the SCCs. The Court was clear that the far-reaching US surveillance laws are in conflict with EU fundamental rights. The US limits most protections to "US persons", but does not protect the data of foreign customers of US companies from the U.S. intelligence services. As there is no way of finding out if you or your business are under surveillance, people also have no option to go to the courts. The CJEU found that this violates the "essence" of certain EU fundamental rights.

The Court has also clarified that EU data protection authorities (DPAs) have a duty to take action. The Court highlighted that a DPAs is "required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence". So far, many DPAs have taken the view that they have unlimited discretion to look the other way. The Court has now put an end to this practice. More information here.

The message by the Court goes beyond the matter of EU-US data transfers in our view. The CJEU has made it clear, that while large parts of the industry and even some Data Protection Authorities look the other way or continue to see the right to data protection merely as "nice to have", the CJEU is willing to send shock waves across the industry and even across the Atlantic, when there is substantial non-compliance.

In order to enforce this judgement by the Court of Justice and urge companies and regulators to comply with the ruling, **noyb** filed more than 101 follow-up complaints against controllers still forwarding data to the U.S in August 2020.

3.1.2. JURIDICAL REVIEW AGAINST THE DPC

Furthermore, **noyb** is forcing the Irish Data Protection Commissioner (DPC), the responsible authority for Facebook, to enforce the judgment by requesting a clear outline of steps that they will take to implement the CJEU's judgement. In its first response on the matter, the DPC refused to outline such steps. On 31 August 2020, the DPC informed **noyb** in a letter that it will open a second case (independent from the complaints procedure that lead to the judgment of the CJEU) to investigate Facebook's reliance on the Standard Contractual Clauses (SCCs). At the same time, the DPC decided to pause the ongoing complaints procedure initiated by Mr Schrems seven years ago, despite being under an undertaking to the Irish High Court from 2015 to decide on the case swiftly.

In response to this situation, the Solicitor representing Max Schrems sent a letter to the DPC, highlighting that the DPC is clearly in breach of a court order by (once more) pausing the complaints procedure from 2013, just to open an unnecessary second investigation into only a sub-issue of the initial complaint.

Mid-September the Irish High Court has granted Facebook leave to file a Judicial Review against the DPC aiming to block the second investigation. Only one months later, the Irish High Court allowed a Judicial Review by **noyb** that aims to swiftly implement the CJEU's judgment and continue the initial procedure, in order to stop Facebook's data transfers to the US.

Hearings for the Facebook case took place in December 2020, while the DPC settled the case filed by Mr Schrems in January 2021, largely on Mr Schrems' terms - but nevertheless delaying the case for almost another year again.

3.1.3 MASS COMPLAINT ON EU-US DATA TRANSFERS

Due to the lack of enforcement of the Schrems II judgment by the relevant authorities, **noyb** filed 101 complaints against several EU/EEA companies with several DPAs against controllers using Google Analytics or Facebook Connect and transfer data to the US without a valid legal basis. As both Google and Facebook are subject to US surveillance laws and must disclose data of European users to US intelligence services, the continued use of Google Analytics and Facebook Connect is illegal. The 101 complaints lodged by **noyb** were therefore intended as a wake-up call: the ruling of the highest Court of the EU must be respected; both data exporters in the EU and data importers in the US have to inspect critical data transfers and, if necessary, stop them. If they do not do so voluntarily, the CJEU has explicitly placed the European Data Protection Authorities under an obligation to prohibit such data transfers.

Results

There was only little reaction from the companies concerned. Only three controllers from Liechtenstein took immediate action and removed Facebook Connect from their webpages. A few other controllers followed their example months later and deactivated the use of Google Analytics or Facebook Connect. **noyb** therefore withdrew a couple of complaints. The pending complaints lead to a specific task force of the European Data Protection Board (EDPB) that provided the DPAs with a set of 26 questions that controllers must now reply when submitting their statements on the complaints.

3.1.4 FAQS FOR CONTROLLERS AND USERS

In addition to the mass complaints, **noyb** provided information for EU companies on how to comply with the ruling and information for users about their options to stop data transfers to the U.S. The first step is to ask companies if and on what legal basis data is transferred. Since the CJEU ruling on EU-US data transfers and especially the lack of a grace period overwhelmed controllers, **noyb** summarized the most common questions and answers by controllers and drafted recommendations for next steps.

Results

We highlighted the possibility to ask companies whether the transfer data to the U.S. and how they comply with the ruling. Many people forwarded **noyb** responses they received from controllers: Some companies like Airbnb, Netflix, and WhatsApp didn't reply to the requests for information at all, while other companies simply redirected to their privacy policies, which lacked more detailed explanation. Others provided information that does not really lead to more certainty, all answers can be found in this report.

3.1.5 FEEDBACK ON FUTURE DATA TRANSFER MECHANISMS

Following the CJEU "Schrems II" judgment which invalidated the Privacy Shield, the European Commission released a revised draft of their Standard Contractual Clauses ("SCCs") for transatlantic data flows on November 12th. The updated draft of the SCCs provides a more comprehensive approach to data transfers and includes four different transfer scenarios.

noyb submitted comments on the Commission's draft SCCs, and in particular expressed concerns with the notion of a so-called "risk-based approach" which some stakeholders read into the Commission's proposal. In addition to these comments, representatives of **noyb** were participating in hearings and discussions on data transfer mechanisms.

3.2 Mobile tracking

In 2020, we filed three complaints regarding the matter of mobile tracking: two against Apple's tracking ID "IDFA" and one against Google's tracking code, as both tech giants fail to comply with EU privacy laws. While most people use their smart phones daily to surf the internet, do research or use apps, it is unclear which activities are tracked by means of built-in unique identifiers that allow various subjects to know our actions and take advantage of our preferences.

3.2.1 COMPLAINT AGAINST GOOGLE'S ANDROID ADVERTISING ID

In May 2020, **noyb** filed a formal GDPR complaint against Google about the so-called "Android Advertising ID", used by Google and third parties (app developers) to track users' actions within and beyond the mobile ecosystem. Our investigation showed that the Android user has no real control over the ID. In particular, Google does not allow to delete it, just to create a new one. The complaint, filed on behalf of an Austrian citizen with the Austrian Data Protection Authority (DPA), focused on the violation of Art. 17 GDPR. The action is partially based on the report "Out of control" by Norwegian Consumer Council. The Austrian DPA may involve other European DPAs in the case.

Results

In June 2020, the Austrian DPA communicated that investigations would have been launched against both Google U.S. and Ireland. In August 2020, **noyb** filed a submission highlighting that Google U.S. is the real controller of the processing and requested to continue the proceeding against this company only. In September 2020 the DPA confirmed receipt of **noyb** submissions. The Austrian DPA is running the investigation.

More information here.

3.2.2 COMPLAINT AGAINST APPLE'S IDENTIFIER FOR ADVERTISERS

Each iPhone runs on Apple's iOS operating system. By default, iOS automatically generates a unique "IDFA" (short for Identifier for Advertisers) for each iPhone. This identifier allows Apple and all apps on the phone to track a user and combine information about online and mobile behavior.

After its creation, Apple and third parties (e.g. applications providers and advertisers) can access the IDFA to track users' behaviour, elaborate consumption preferences and provide personalised advertising. Such tracking is strictly regulated by the Article 5(3) of the e-Privacy Directive and requires the users' informed and unambiguous consent.

Apple operating system places these tracking codes without the knowledge or agreement of the users.

On November 16, 2020 **noyb** assisted two data subjects based in Berlin and Madrid in filing a complaint against Apple before the Data Protection Authority in Berlin and the Spanish Data Protection Authority in cooperation with Xnet.

Since this complaint is based on the e-privacy directive and not GDPR, the relevant authorities in Germany or Spain could decide to directly fine Apple without cooperation with Ireland, where Apple's European headquarter is located.

Results

The Spanish DPA has received the case and is currently running the investigation. The Berlin DPA transmitted the case to the Bavarian DPA where Apple Germany headquarters are located. **noyb** is waiting for an update from the Bavarian DPA. These complaints have been widely reported in international media (e.g. Reuters, El Mundo, The Guardian and many more.)

More information here.

PHOTO BY SHAHADAT RAHMAN / UNSPLASH

3.3 Encryption

Emails always contain personal data. During their route toward the recipient such communications are handled by different entities, nodes and service providers which may intercept, manipulate and unlawfully use their content. In order to reduce these risks, Article 32 of the GDPR requires the controllers to implement appropriate security measures, such as so-called TLS encryption.

3.3.1 COMPLAINT AGAINST AMAZON

noyb submitted a complaint to the supervisory authority of the state of Hessia in Germany on behalf of an Amazon seller, as the GDPR requires companies to implement "appropriate" security measures, such as encryption, to protect the confidentiality of communications. As TLS encryption is very cheap and simple to implement and the number of sellers and customers on Amazon is very high, it seems inappropriate to neither require not allow TLS for emails. Surprisingly, the Amazon servers reject TLS connections in certain cases, for example when third party sellers on Amazon communicate with customers vie email. This means that millions of emails that are sent via Amazon may be exposed.

Results

The Hessia data protection authority transmitted the case to the Bavarian DPA where the Amazon German headquarters are located. The Bavarian DPA has, in turn, involved the Luxembourgish DPA as lead supervisory authority (LSA). The authorities concerned (including the LSA) have conflicting views. The case has therefore been referred to the EDPB for its opinion.

More information here.

3.4 Data Subject Rights

The General Data Protection Regulation (GDPR) grants people a range of data subject rights. Through these rights, data subjects can make a specific request and be assured that personal data is not being misused for anything other than the legitimate purpose for which it was originally provided. As controllers do not always comply with this essential part of the GDPR, noyb has filed several complaints on behalf of data subjects for violations of data subject rights, specifically the right to access (Article 15 GDPR) and the right to rectification (Article 16 GDPR). Furthermore, noyb has started an awareness campaign to guide users how they can make use of their GDPR rights.

3.4.1 COMPLAINT AGAINST A1 TELEKOM AUSTRIA

In June 2020, **noyb** filed a GDPR complaint against A1 Telekom Austria, as A1 refused to provide traffic and location data to its customers after submitting an access request (Article 15 GDPR). Since A1 also uses this data for movement analyses (recently for corona analyses), the lack of transparency seems particularly problematic.

The complaint focuses on "location data" and "traffic data". The former is data indicating the geographical location of the telecommunication equipment of a user; it can therefore be used to determine the location of a user's mobile telephone. The latter, includes IP addresses, log data, time and duration of the connection, the amount of data transmitted and certain location data. A1 only provides this traffic data as part of the bill including itemised billing, although the GDPR entitles the user to receive a copy of all their personal data at any time.

Results

A1 has defended their point of view before the Austrian DPA, which announced to issue a decision soon.

More information here.

3.4.2 COMPLAINT AGAINST ADDRESS BROKER AZ DIRECT GMBH

Mid-October 2020 **noyb** filed a complaint against AZ Direct Österreich GmbH with the Austrian DPA. The company, which belongs to the Bertelsmann group, had refused to provide information on the origin and recipients of the data processed. The data subject had sent an access request under Article 15 GDPR to AZ Direct. He also asked from where the address publisher had collected his data and to whom it had been sold.

AZ Direct stated that it had stored (former) residential addresses of the data subject but did not provide any detailed information on the origin of the data – although the GDPR explicitly requires this.

According to the GDPR, the reply to an access request must also contain information on who the recipients of the data were. AZ Direct remains silent in this regard as well and only gives possible categories of recipients but refuses to say to whom exactly which data was transmitted. Nevertheless, data is collected and sold to advertisers.

Results

AZ Direct had replied to **noyb**'s complaint and insisted on their point of view that they do not have to provide the data subject with further information on data sources and recipients. The Austrian DPA has announced to issue its decision in due time.

More information here.

3.4.3 COMPLAINT AGAINST WIZZ AIR

Under Article 16 GDPR (Right to Rectification), users have the right to have inaccurate or incomplete personal data rectified, without undue delay. This way, personal data is not only protected, but is also accurate.

In October 2020, **noyb** filed a complaint against Wizz Air, Central and Eastern Europe's Largest Low Cost Airline. After changing her surname and consequently her email address, an Austrian passenger of Wizz Air needed to update her data stored with the company. As the passenger couldn't do this herself, she filed a "rectification request" for her surname and email address with Wizz Air's Data Protection Officer (DPO). Three months later, the passenger still had not received any response. She submitted a new request to change her surname using the company's contact form. Customer Service told her that she could not change her surname online except in case of marriage. In her case, she would need to call the Wizz Air Call Center, which costs more than 1 Euro per minute. After an unnecessarily long procedure, and despite the free right of rectification under the GDPR, the airline charged 35€ in phone charges to update her surname. The corresponding e-mail was never changed, which meant that e-mails from Wizz Air were not delivered and the passenger almost missed her flight.

The GDPR gives customers the right to correct their information free of charge (Article 12(5) GDPR). By forcing customers to call their expensive hotlines to rectify inaccurate data, Wizz Air fails to let customers exercise this "right to rectification".

Results

In December 2020, the Austrian Data Protection Authority (DPA) informed **noyb** that the cooperation mechanism had been triggered between Austria and Hungary with the complaint was forwarded to the Hungarian DPA.

More information here.

3.4.4 NOYB'S EXERCISE YOUR RIGHTS SERIES

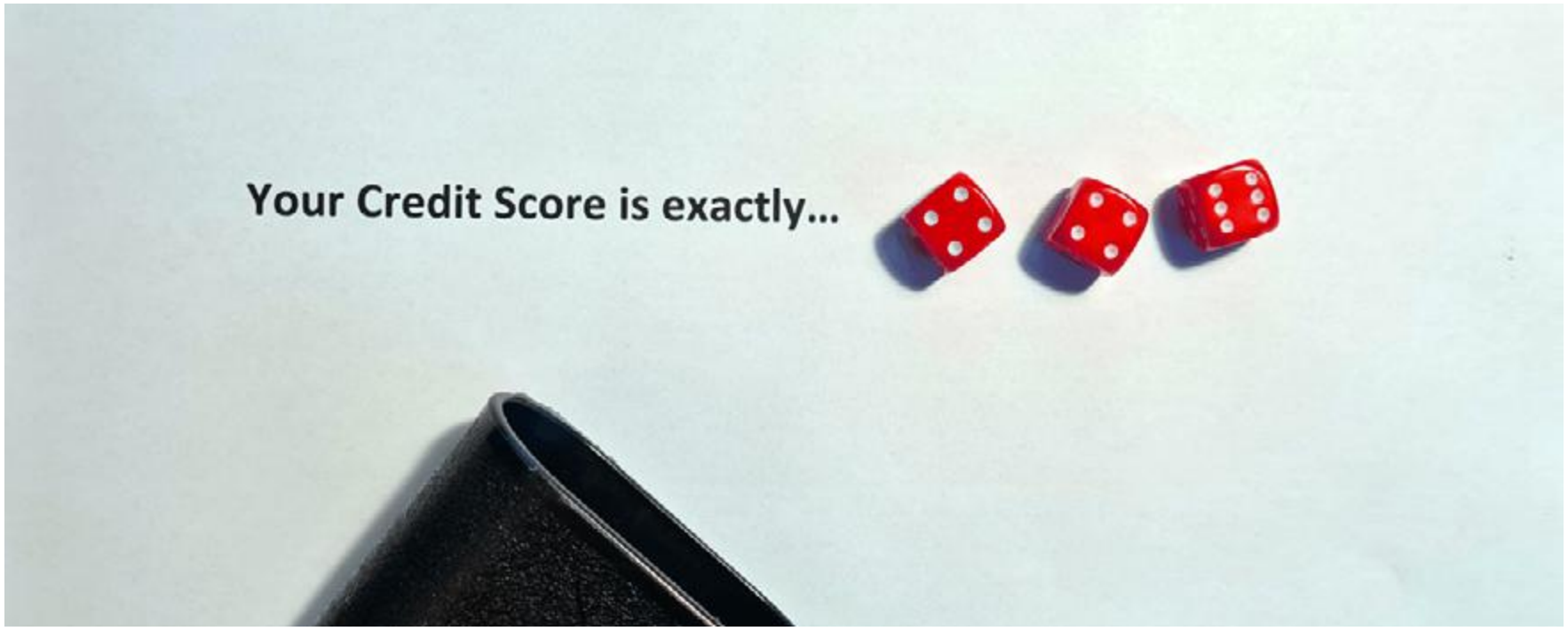
We experience that users are not always well informed of their rights under the GDPR and how to ask organisations if they uphold these rights. The campaign "Exercise your Rights" was launched to inform the public about how they can concretely ask the controllers to access, correct, delete or stop processing their data, or to obtain the delisting of their name in a search result.

Each page focuses on a specific right under the GDPR and explains concretely how to write a request to the relevant controller. The main objective of the series is to provide for basic information in a plain language for users without legal background.

More information here.

3.5 Credit Ranking Agencies

Credit ranking agencies sometimes have great power over consumers and have so far shown little responsibility in exercising this power. Often they follow national traditions instead of the GDPR, which has been applicable throughout Europe since 2018.



3.5.1 COMPLAINT AGAINST CREDIT RANKING AGENCY CRIF

In August 2020, **noyb** filed a GDPR complaint against the credit ranking agency "CRIF".

An electricity customer wanted to sign a new electricity contract. The energy supplier unexpectedly refused to sign the contract because the customer's credit ranking was too low. In response to further inquiries, it was explained that his "CRIF credit score" would only be 446 points, while the minimum requirement for an energy contract was 650 points. The customer then approached CRIF and requested access to his personal data under Article 15 GDPR. Surprisingly, CRIF responded by claiming that it has not stored any personal data on him.

Nevertheless, CRIF assigned a "score" of exactly 446 out of 700 possible credit points to the debt-free electricity customer with a well-paid permanent job. Due to the lack of information and the obviously incorrect data, **noyb** has filed a complaint with the competent Austrian data protection authority.

Results

CRIF has replied to **noyb**'s complaint and again refused to shed a light on their opaque processing activities. It is now up to the Austrian DPA to decide the case in a timely manner.

More Information here.

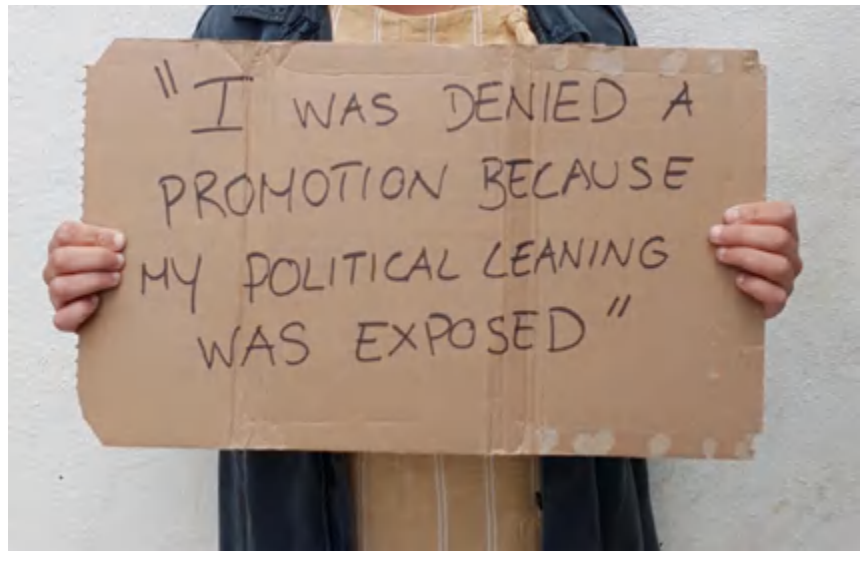
3.6 Data breaches

We happen to deal with data breaches with a large impact on the individuals' rights and freedoms. Data breaches can reveal that a secret processing took place and that organisations were not complying with the GDPR.

3.6.1 COMPLAINT AGAINST IT SOLUTIONS "C-PLANET"

In April 2020, following a data breach, a large majority of Malta's voters found their personal data available online: the leaked information included their phone numbers, dates of birth and political opinions. After having been contacted by the NGOs Daphne Foundation, **noyb** filed a complaint with the Maltese DPA, on behalf of several Maltese citizens. One of the request of the complaint was to investigate on the company responsible for the leaked database of voter's data in Malta: C-Planet IT Solutions, which appears to be connected to the Labour Party, in government in Malta since 2017.

In parallel, the NGOs Daphne Foundation and Repubblika initiated a class action on behalf of the citizens affected by the data breach.



More information here.

3.7 Knowledge Sharing

Besides working on complaints, noyb is also actively disseminate GDPR developments to professionals and the general public, notably through our public wiki GDPRhub and the newsletter GDPRtoday.

3.7.1 GDPRhub AND GDPRtoday

In October 2019, **noyb** initiated a newsletter project with the aim to cover decisions issued by European DPAs and Member State and European courts. For this purpose, **noyb** created a database with all the national sources across Europe for DPA and court decisions and employed a tool for monitoring them and creating notifications about any updates. After preparatory work was completed, GDPRhub and GDPRtoday were started in February 2020: a free and open wiki that allows anyone to find and share GDPR insights across Europe, together with a newsletter showcasing recent additions and commentary on privacy developments.

By the end of 2020, more than 650 decisions were listed on GDPRhub, less than 12 months after its launch, and more than 3,900 subscribers receive the weekly GDPRtoday newsletter.

The content on GDPRhub is divided into two databases: decisions and knowledge. The decisions section collects summaries of decisions by national DPAs and European and Member State courts in English. The knowledge section lists commentaries on GDPR articles, DPA profiles, and 32 GDPR jurisdictions (EU + EEA). More than 60 volunteers assist us in the collection of these sources in jurisdictions which **noyb** could not cover in-house due to language barriers.

3.8 Research

3.8.1 REPORT ON STREAMING SERVICES

Together with the Austrian Chamber of Labour (Arbeiterkammer), **noyb** investigated the information practices of eight streaming services against provisions of the GDPR: Amazon Prime, Apple Music, DAZN, Flimmit, Netflix, SoundCloud, Spotify and YouTube. The GDPR requires providers to give information on the use of personal data and the data protection rights of users "in a precise, transparent, comprehensible, easily accessible form and in plain language". The test shows: What happens to customer data often remains in the dark. AK and **noyb** assessed eleven requirements of the GDPR. In general, information was often unclear or simply not given.

Regarding the transfer of personal data to recipients, a category a lot of users are curious about, only Flimmit stated which personal data is transferred to which category of recipients and for what purpose – though here, too, the specific recipients were mostly missing. In summary: Services mostly fail in complying with one of the GDPR's most basic requirements - namely that users are informed about what happens to their data.

More information here.

3.8.2 REPORT ON PRIVACY POLICIES OF VIDEO CONFERENCING SERVICES

Video conferencing tools literally open a lens into our homes. The personal and professional spheres are increasingly merging. **noyb** examined the privacy policies of six tools: Zoom, Webex Meetings (Cisco), Meeting (LogMeIn), Skype and Teams (both Microsoft), and Wire. While the video quality of the investigated tools may often be crystal clear, and the user interfaces well-thought out, the service providers'

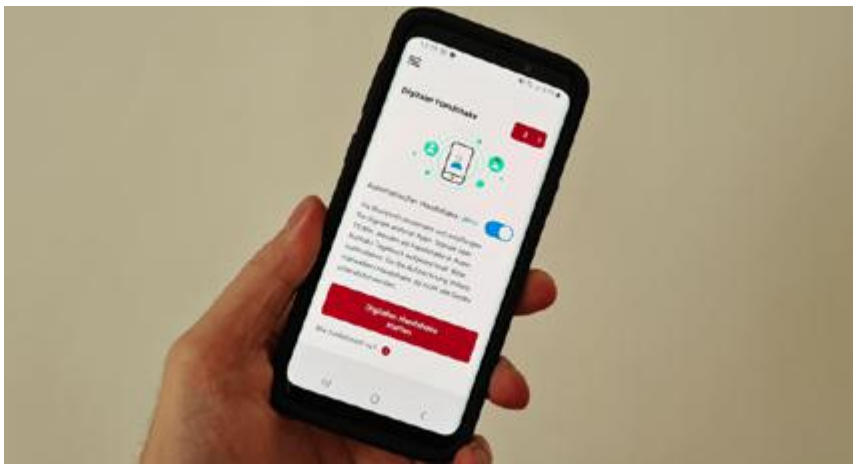
OVERVIEW OF THE SELECTED INFORMATION OLIGATIONS UNDER ARTICLE 13 GDPR

✓ mostly satisfactory ◉ partly satisfactory ✗ not satisfactory

Information according to Article 13 GDPR	Zoom	Webex Meetings (Cisco)	GoToMeeting (LogMeIn)	Skype (Microsoft)	Teams (Microsoft)	Wire
Identity and contact details of the controller	✓	◉	◉	✓	✓	◉
Contact details of the DPO	✓	✗	◉	◉	◉	✓
Purposes of processing	✓	✓	◉	◉	◉	◉
Legal basis for processing	✗	✗	✗	◉	◉	✓
In case of legitimate interests: What are the interests of the controller or third parties?	✗	Not applicable	✗	◉	◉	◉
Interconnection: categories of personal data, purposes, and legal bases	✗	◉	◉	✗	✗	✓
Recipients or categories of recipients of the personal data	◉	✗	✗	✗	✗	✗
Transfers outside of the EU/EEA	✗	✓	◉	✗	✗	✗
Retention periods	✗	✓	✗	✗	✗	✓
GDPR right to withdraw the consent	✓	✗	◉	✓	◉	✓
GDPR right to lodge a complaint	✓	✗	✓	◉	◉	✗
Existence of automated decision making	◉	◉	◉	✓	✓	◉

privacy policies do not meet this standard. Static in the form of “may” or “might”, “as necessary”, or “as required by law” cloud the picture. Sometimes whole parts are missing, such as information about basic GDPR rights. Finally, poor structure makes accessing the available information challenging.

More information here.



3.8.3 REPORT ON SARS-COV-2 TRACKING UNDER GDPR

In the past year, the discussions around the use of data to combat the corona pandemic have constantly increased. Therefore, we wrote a report on compliance with the GDPR and legal requirements for virus tracking apps. Contrary to many initial reports, there is no general conflict between data protection (especially the GDPR) and the use of personal data in the fight against an epidemic. While this paper can give a general and superficial overview of the minimal requirements of the GDPR and possible compliance strategies, it naturally remains abstract and needs to be adapted to any specific tracking project. We feel that compliance with baseline privacy protections is crucial for the acceptance of any such tracking system by the public.

More information here.

3.8.4 REVIEW OF AUSTRIAN “STOPP CORONA APP”

The Austrian Red Cross published an initial version of a “Contact Tracing App” on March 25th. Together with epicenter.works and SBA research, **noyb** reviewed Europe’s first Corona App.

After reviewing the source code, we had the impression that many of the requirements for the app were only added after the start of development (e.g. automatic handshake). Although a privacy friendly approach has always been followed, the additional requirements and technical limitations on the smartphone operating systems of Google and Apple led to an architecture that has certain problems. Our code review identified some serious privacy issues, some of which have already been taken care of by applying a hotfix. From a legal perspective, we have some suggestions for improvement, but in our opinion the concept of the app is compliant with data protection laws. The technical security check did not reveal any critical security vulnerabilities, but some suggestions for improvement were made.

More information here.

3.9 Updates on past projects

noyb is continuously pushing forward already filed complaints and ongoing proceedings. In 2020, a few decisions were made and some fines were imposed, in other projects only little progress was achieved by the responsible authorities.

3.9.1 STREAMING COMPLAINTS

In cooperation with the Austrian Chamber of Labour, **noyb** filed eight complaints against streaming services such as Netflix and Amazon Prime in January 2019 for not sufficiently complying with the right of access under Article 15 GDPR. A first decision was issued in September 2020 – more than one and a half years after the complaint was lodged – the Austrian data protection authority (DSB) decided on the complaint against the Vienna streaming service Flimmit. The legal deadline for decisions in Austria is six months. The DSB took its decision only after **noyb** filed a so-called late complaint with the court, giving the DSB three months to take a decision.

PHOTO BY GLENN CARSTENS PETERS / UNSPLASH

On the merits of the case, the DSB rejected **noyb**'s complaint. The rejection was only based on the fact that Flimmit submitted the information that was missing from the original information provided (namely, to whom the complainant's data had been transmitted) in the course of the DSB procedure. Such "ex-post compliance" by a data controller allows the DSB to close complaint procedures without having to examine whether there was a GDPR-violation.

At the same time, it allows companies to comply with the GDPR only in the event of a complaint and still escape without any fine. There is little progress on the other streaming complaints (against Amazon Prime, Apple Music, DAZN, Flimmit, Netflix, SoundCloud, Spotify and YouTube). In the case against DAZN, **noyb** has also filed a complaint due to the DSB's inactivity with the Federal Administrative Court. In that case, the DSB was unable to make its decision within three months and has handed the case to the Federal Administrative Court. With regard to YouTube, there is disagreement as to which authority is responsible. Other procedures seem to simply have been lost, although **noyb** keeps following-up with the authorities. Of eight proceedings, only one has been decided after more than one and a half years.

More information here.

3.9.2 FORCED CONSENT - GOOGLE

On 19 June, the Conseil d'Etat (the French highest administrative court) upheld the French Data Protection Authority's (CNIL) jurisdiction and decision to impose a 50 million euro fine on Google over the company's opaque privacy policy and lack of legal basis for personalized ads.

Following a complaint by **noyb** and a similar complaint by the French NGO "La Quadrature du Net" the CNIL imposed a 50 million euro fine on Google over the company's opaque privacy policy and lack of legal basis for personalized ads. The decision was appealed by Google before the French Conseil d'Etat on the grounds that the French DPA doesn't have jurisdiction over Google's European headquarters. Google claimed, among others, that the Irish data protection authority should be leading any cases or investigations into its practices. The Conseil d'Etat upheld the decision of the CNIL in all points.

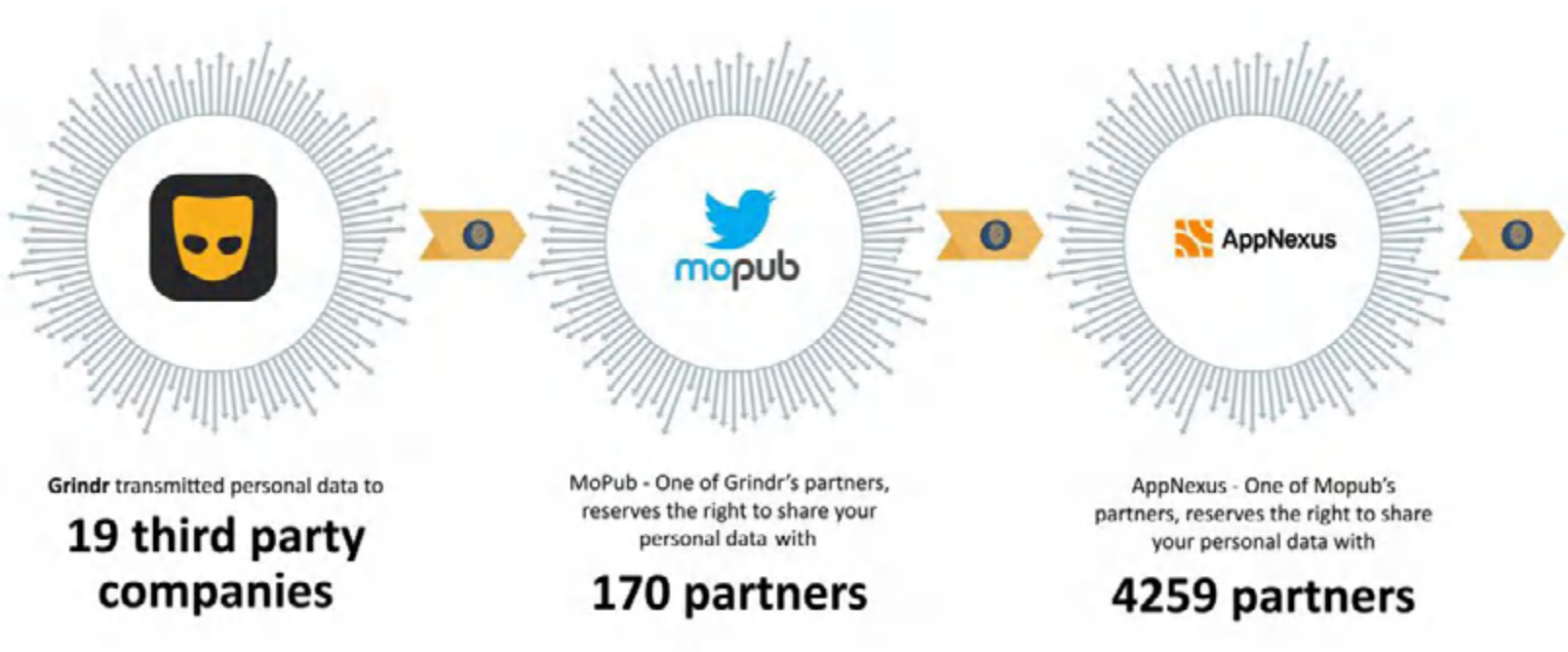
More information here.

3.9.3 GRINDR

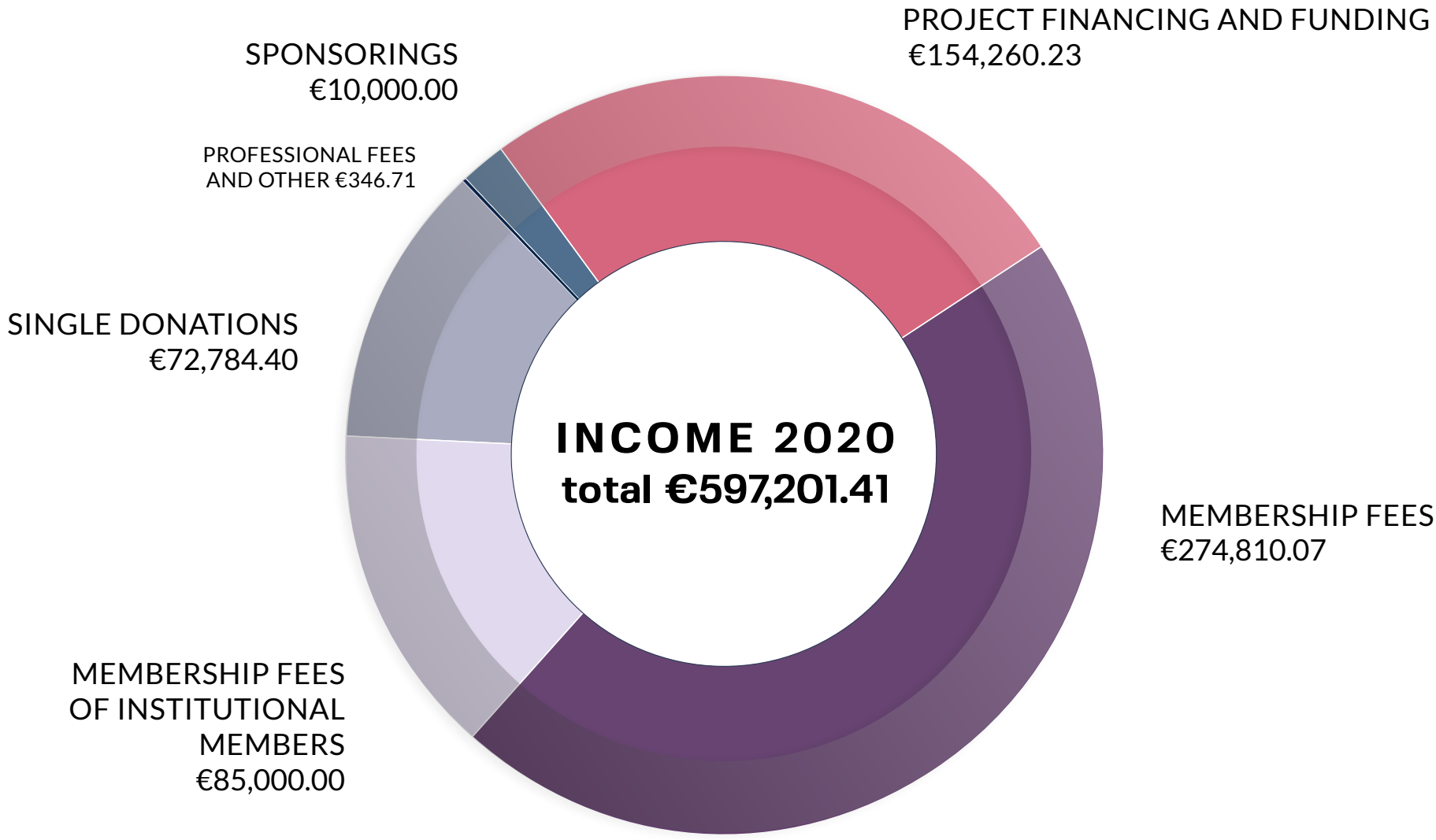
Together with the Norwegian Consumer Council, **noyb** filed [three strategic complaints] against the dating app Grindr and several adtech companies over illegal sharing of users' data in January 2020. Like many other apps, Grindr shared personal data (like location data or the fact that someone uses Grindr) to potentially hundreds of third parties for advertisement.

One year after the complaint was filed, the Norwegian Data Protection Authority upheld the complaint against Grindr, confirming that Grindr did not receive valid consent from users in an advance notification. The Authority imposes a fine of 100 Mio NOK (€ 9.63 Mio) on Grindr. An enormous fine, as Grindr only reported a profit of $ 31 Mio in 2019 - a third of which is now gone.

More information [here.]

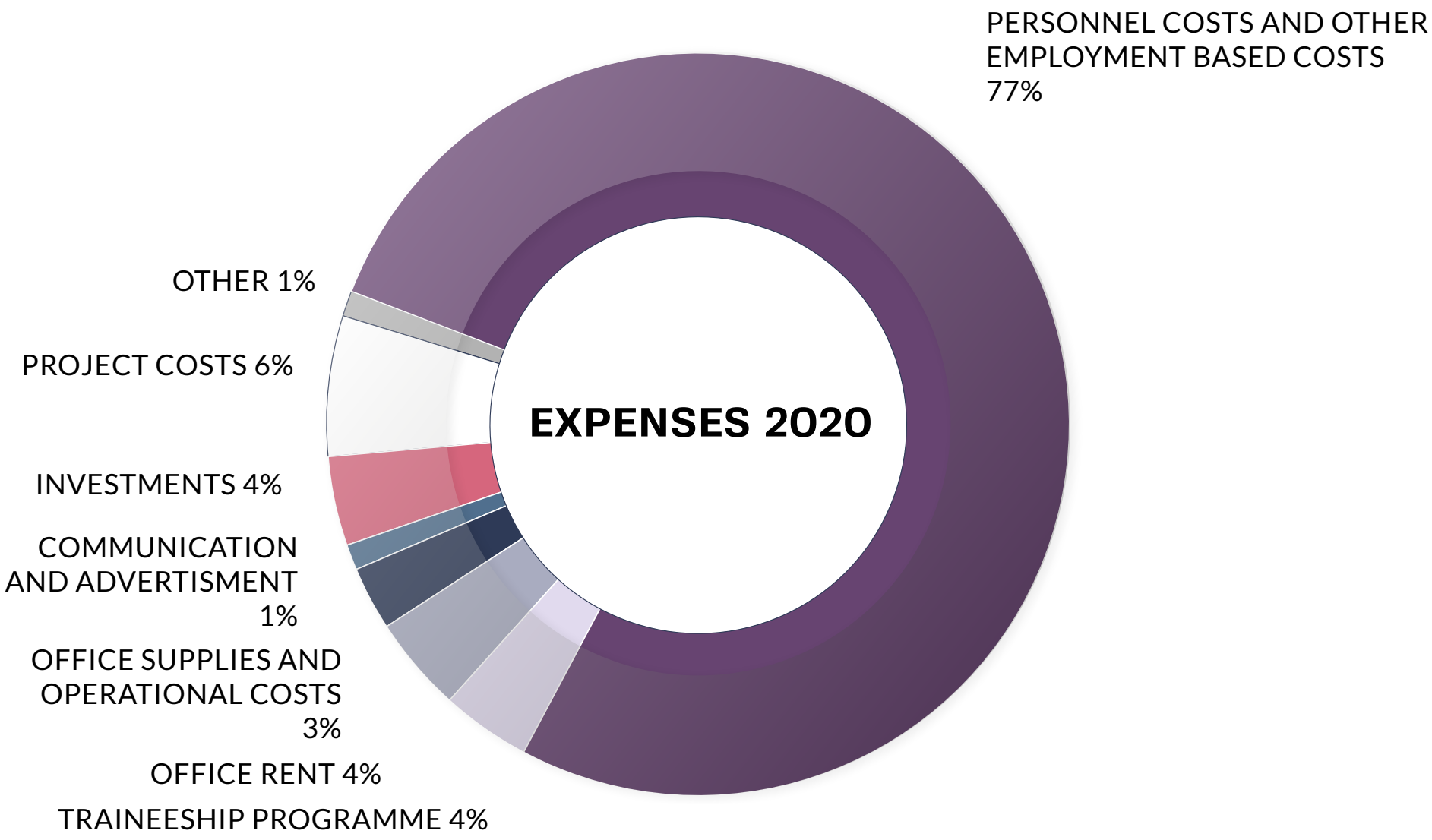


Finances 2020



- MEMBERSHIP FEES: fees from 3.716 individual supporting members
- MEMBERSHIP FEES OF INSTITUTIONAL MEMBERS: City of Vienna (€ 25.000), Austrian Chamber of Labor (€ 60.000 – payment for 2018, 2019, 2020 of € 20.000 each received in 2020)
- SINGLE DONATIONS: individual donations ranging from € 1 to € 20.000 by individuals or SMEs
- PROFESSIONAL FEES AND OTHER: no speaking fees in 2020, interest
- SPONSORINGS: Surfboard Holding BV (€ 10.000)
- PROJECT FINANCING AND FUNDING: core funding by the Austrian Federal Ministry of Social Affairs, Health, Care and Consumer Protection (€ 16.500), Forbrukerradet (€ 11.308,51), Open Society Foundation (€ 68.454,41), Austria Wirtschaftsservice GmbH *"NPOfonds"* (€ 57.997,31)

Finances 2020



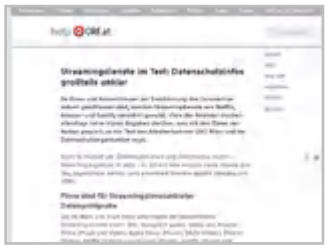
As noyb is mostly financed by private supporters and public entities, we want to report our incomes and expenses as transparently as possible. For strategic reasons we decided to disclose only our income numerically and use percentages for our expenses. In our first two years we put aside a substantial sum to a reserve fund for future court fees and alike which is therefore not part of our budget. The sum in our reserve fund would be of great strategic importance for our opponents, who are typically very well-funded and have, compared to us, limitless resources, and can therefore not be disclosed. Thank you for your understanding!

- PERSONNEL COSTS: salaries, ancillary wage costs, travel costs, training costs and payroll accounting
- TRAINEESHIP PROGRAM: housing, public transportation and daily allowances for trainees
- PROJECT COSTS: legal fees for projects, costs for GDPRtoday
- INVESTMENTS: furniture, IT equipment, literature, software and alike
- OTHER: bank fees, membership fees (EDRi), depreciation

noyb in media

With over 275 mentions in media outlets, we reached both national and international audiences.

Here are some of our highlights of 2020.



The Austrian Broadcasting Corporation (ORF) on our Streaming

Profil on our analysis of the "Stopp Corona App"

Bloomberg and TechCrunch on our complaint against Google's tracking ID

Reuters and RTE News on our Open letter to the Data Protection Commissioner

derStandard and Profil on the fine against Google

The Irish Times and TechCrunch on the CJEU Judgment on EU-US data transfers

TAZ on our 101 complaints against major EU websites defying the CJEU Judgment

The Wallstreet Journal on our future class action filings in Belgium

The Associated Press on our complaint against Apple's tracking Code IDFA

The IAPP on our complaint against Wizz Air

noyb European Center for Digital Rights

noyb in numbers

2020

TEAM MEMBERS

11

FROM 8 DIFFERENT COUNTRIES

LEGAL TRAINEES

10

FROM 8 DIFFERENT COUNTRIES

SUPPORTING MEMBERS

3716

FROM 45 DIFFERENT COUNTRIES

110 COMPLAINTS AGAINST 109 COMPANIES
FILED IN 19 COUNTRIES, REPRESENTING 110 DATA SUBJECTS

2 FINES
€60,000,000
IN TOTAL

280,150
UNIQUE VISITS TO OUR WEBSITE

THE BUSIEST DAY ON OUR WEBSITE: 16TH JULY 2020
18,673 visits

ARTICLES AND MENTIONS
OVER 275

IN TOTAL
27,565 FOLLOWERS ON SOCIAL MEDIA

25
PRESS RELEASES

12
NEWSLETTERS

European Center for Digital Rights

noyb – European Center for Digital Rights

Goldschlagstraße 172/4/3/2
1140 Vienna – Austria
ZVR: 1354838270