
# *Making Privacy a Reality*

Public Project Summary

**EXECUTIVE SUMMARY**

# *#MakingPrivacyAReality*

**Europe has stringent privacy and consumer protection laws, but lacks enforcement in the area of digital rights. Consequently, there is a huge gap between privacy protections on paper and in real life. The aim of NOYB is to close this gap - and make privacy a reality.**

---

**Promising Experiences.** Recent individual legal enforcement actions show that even rather simple cases prove successful in courts and lead to substantial shifts towards more privacy protection in everyday life. Notable examples are the European Court of Justice (CJEU) rulings regarding the EU data retention directive, the "right to be forgotten" ruling or the invalidation of "Safe Harbor" on EU-US data transfers.

**Professionalizing.** It is time for a professional and strategic enforcement organization, that operates on a European level, to tackle widespread privacy violations and bring meaningful privacy protections to the daily life of citizens throughout the European Union and beyond.

**Strategic and Effective.** The aim of NOYB is to positively impact the daily privacy of as many citizens as possible, using the most effective enforcement options. Novel approaches to EU privacy litigation, from automatization (legal tech), crafting of ideal model cases in the most effective jurisdiction (strategic litigation) and privacy "class actions" (collective enforcement) to intensive cooperation with existing structures shall be utilized to pursue this aim.

**Cooperation.** NOYB will liaise with existing consumer rights organizations, advocacy NGOs or critical tech organizations to use and coordinate existing expertise on a European level ("*hub function*") for enforcement actions. NOYB will, at the same time, develop the necessary capabilities to compliment these existing resources and fill gaps in individual cases.

**Quality Assurance.** In cooperation with other organizations NOYB shall provide its specialized knowledge on data protection and strategic litigation and thus raise the substantial quality of litigation projects in this field. At the same time NOYB can prevent the potential abuse of data protection litigation instruments by questionable actors (e.g. abusive for-profit litigation or misuse by competitors).

**Focus on Commercial Privacy.** NOYB will focus on commercial data protection and related consumer rights (not government surveillance), for two reasons: First, EU civil law allows pan-European strategic litigation in the commercial sector, while government surveillance usually has to be challenged nationally. Second, existing groups in many member states are already active in the area of government surveillance, while enforcement in the commercial sector is rather limited.

**Crucial Moment.** On May 25th 2018 the European General Data Protection Regulation ("GDPR") comes into force. The GDPR foresees dramatically improved enforcement mechanisms, including emotional damages, options for collective redress and sanctions of € 20 million or 4% of the global revenue. This shift is aimed at making privacy and data protection a serious compliance and legal issue for the industry.
At the same time the judiciary, including Court of Justice of the European Union ("CJEU"), is currently willing to issue stringent judgements in the area of privacy and data protection.

**European Scope, Global Impact.** Most relevant IT providers act on a pan-European or even global level. At the same time the new European General Data Protection Regulation ("GDPR"), applies to any operator that targets the European market. Jointly this allows strategic privacy litigation on a European level.
While EU law only applies to the European market, global providers that offer "one size fits all" solutions will often have to stick to the highest global standard in practice. Many global providers also operate EU subsidiaries for non-EU markets (e.g. EMEA or all non-US markets). Europe can therefore function as a global pacemaker ("*California Effect*"), leading to a higher level of privacy protections worldwide.

**Optional Broadening.** NOYB may broaden the scope towards other areas of digital rights (copyright, freedom of speech, net neutrality) in the long run. Currently NOYB aims to cooperate with other NGOs in these areas, especially when they pursue privacy-related cases.

**Experienced Team & Members.** NOYB was initiated by *Max Schrems*, an Austrian lawyer who brought down the EU-US "Safe Harbor" agreement. The board of NOYB also include: *Christof Tschohl, data* protection expert and lawyer behind the successful Austrian challenge against the European Data Retention Directive (C-594/12) and *Petra Leupold,* consumer rights expert, lawyer at the Austrian Consumer Rights Organization ("VKI") and head of VKI academy.
Members of NOYB consist of recognized experts in the area of data protection, consumer law and technology, including *Jan-Philipp Albrecht* (Member of the European Parliament, Rapporteur on GDPR) or *Paul Nemitz* (Director - Fundamental Rights , European Commission).

**Key Facts.**

| | |
|---|---|
| Name: | NOYB |
| Legal Structure: | Austrian Non-Profit ("*Verein*"), established 06/2017 |
| Location: | Vienna, Austria |
| Governance: | Members > Board of Directors > Managing Director |
| Proposed Core Staff: | 5 full-time |
| Proposed Core Budget: | € 500.000 p.A. |

# TABLE OF CONTENTS

# CHAPTER 1: VISION

- Challenge
- Proposed Solution
- Beneficiaries
- Guiding Principles

# 1.1. CHALLENGE

**Privacy.** The transition to an information society is as fundamental as the previous shift to an industrialized society. This transition makes it essential that citizens can enjoy the benefits of new technology, while ensuring that new technologies and services serve the people. The rights to data protection and privacy are aimed at giving citizens the necessary control over their information. It is the pillar to ensure trust in new technology and a transition that benefits the whole society.

**Law = Reality?** Europe has a robust and clear legal framework for the protection of the fundamental rights to privacy and data protection - but, in reality, these rights are not respected by large parts of the tech industry. We witness regular revelations, public outrage and a constant debate - none of shich impact on actual practices. This gap between existing law and our daily reality is mainly the result of an absence of enforcement.

**Lack of Enforcement.** Private actions by consumers are rare because of a lack of knowledge of rights, complicated procedures, costly cases and little financial benefits from pursuing cases individually. The existing data protection authorities (DPAs) often lack resources, expertise and initiative to uncover and prosecute violations of the law.

**Existing NGOs.** So far no institution is aiming to close this gap on a European level. Existing institutions serve important roles in other areas, but do not engage in enforcement in the private sector.

- The focus of European privacy NGOs (mainly EDRI) is policy work. These efforts can be supported by strategic enforcement, especially in politically relevant cases, while NOYB will itself not engage in policy work.
- Most existing national NGOs and activist groups that take legal actions, focus predominantly on government surveillance, while NOYB will focus on commercial privacy violations.
- Some NGOs and law firms in the United States have taken a legal path in the commercial sector, but because of a lack of an omnibus privacy law in the US, the factual impact of these cases was relatively limited.
- Groups of hackers and IT specialists usually have the necessary ability to factually discover misuse of data and produce the necessary evidence, but rarely pursue legal actions.
- Existing consumer organizations often see privacy violations as a side topic, given the wide range of other pressing consumer rights matters. They are often willing to support privacy efforts, but mostly lack the technical and legal expertise in this very specialized field of law.

In summary there is a wide field of existing actors that have valuable individual resources that could be used through cooperation, but none are currently engaging in strategic litigation in the commercial sector on a European level that could close the gap between existing fundamental rights and reality.

**Fair Competition?** We currently see a trend that companies which comply with the law are at an unfair disadvantage over non-compliant players in the same market. Non-compliant competitors usually operate from jurisdictions that lack relevant laws and/or adequate enforcement of privacy regulations - leading to unfair competition.

# 1.2. PROPOSED SOLUTION

**Real-Life Privacy.** Fundamental Rights are not won on paper, but in reality. The aim of NOYB is therefore to ensure that the tech industry is following fully the existing privacy and data protection laws in the European Union, through strategic litigation in the public interest. Just like other areas of law, only the realistic likelihood of enforcement will ensure that laws are generally respected.

**Strategic, Effective and Collective Enforcement.** Privacy violations usually impact a large number of individuals, but only result in relatively small claims per affected person. Cases are usually legally and technically complex, adding to enforcement costs. In reality individuals are organizationally and financially unable to bring cases in these situations. A pan-European strategic and collective enforcement NGO can overcome this situation. NOYB will prioritize relevant cases, ensure that relevant violations are uncovered, assess legal and factual situations and use the most effective form of enforcement in each case. This may include the use of automated legal processes and enforcement ("legal tech").

**Cooperation with Existing Actors.** Many of the necessary resources for the enforcement of privacy violations already exist. For example: Existing hacker organizations are able to uncover wrongdoings, data protection authorities are able to raid companies and consumer rights organizations have expert knowledge in legal enforcement. The proposed organization should therefore primarily connect these resources and trigger actions by existing actors, while at the same time being able to fill gaps in the existing structure whenever needed.

**Using new Options under GDPR.** The European Union has passed the General Data Protection Regulation ("GDPR") which will replace all national data protection laws on May 25th 2018.
The EU has realized that enforcement is key for privacy protection and encourages private action. GDPR foresees collective enforcement by NGOs and has significantly strengthened the redress options for individuals (e.g. emotional damages for each violation). Though strategic complains penalties of up to €20 Mio or 4% of the worldwide turnover of companies can be triggered. The proposed organization would ensure, that these options are used in practice - as foreseen by the legislator.

**Ensuring Fairness on the European Market.** To date it made sense, from a mere economic point of view, to ignore existing laws, because enforcement was almost nonexistent and penalties were trivial. Companies even gained a competitive advantage from ignoring the fundamental rights of individuals. As in other fields of law, solid enforcement will ensure a level playing field for compliant competitors and disincentivize efficient breach of law.

**European Hub.** The proposed organization fills the gap between existing structures. The aim to mainly develop a hub should ensure that no new parallel structures are developed, but existing resources are put to work for privacy enforcement in a strategic and effective way. However, where no adequate structures exist, NOYB shall be able to fill those gaps.

# 1.3. BENEFICIARIES

**Citizens & Consumers.** The main beneficiaries from proper enforcement of the fundamental rights to privacy and data protection are obviously consumers and citizens, whose rights are currently violated by commercial actors on a regular basis. Because the European Union is likely to set the worldwide "gold standard" for privacy, the factual protection may be available to people far beyond the EU.

**Existing NGOs.** Existing European and international NGOs in the policy and advocacy field may benefit from solid cases, uncovering violations and generating results under the current law. Close cooperation is needed to ensure that results are balanced, in line with policy and advocacy objectives and do not generate unwanted backlashes from enforcement actions.
Existing enforcement initiatives could benefit from a reliable European hub, as well as financial, legal and strategic support. International enforcement NGOs, especially in the US, may find it helpful to bring cases against international players in a jurisdiction which is more favorable than their home jurisdiction.

**Authorities.** Data Protection Authorities (DPAs) could benefit from well-researched complaints by NOYB, which limit the workload and may lead to quicker enforcement actions, additional enforcement pressure, as well as information gathering and sharing. Most DPAs are currently not equipped with enough technicians and labs to allow wider research of facts. In addition private actors are also not bound by procedural laws that limit the capabilities of DPAs to investigate, uncover violations or procure evidence, while most procedural laws allow DPAs to use such information once produced by a private actor.

**Industry.** Many companies currently perceive an imbalance between companies who respect the law and others who gain competitive advantages by violating it. While legal limitations and the enforcement thereof are, for the most part, not beneficial for commercial actors, many traditional competitors could benefit indirectly from limiting unfair competition. Privacy friendly alternatives could equally benefit from uncovering violations by current actors, enforcement against them and the promotion of alternatives.

# 1.4. GUIDING PRINCIPLES

**I. Real Life Effects.** The main aim of the proposed organization is to align practices in daily life with the existing law, as well as to bring cases that develop the existing case law further. Most privacy issues are well-known and regulated, but still not enforced in practice.

**II. Effectiveness & Principle of Subsidiarity.** The operation of the proposed organization is designed to have the maximum real-life effect, with the resources available. Most elements necessary for large-scale and successful enforcement (e.g. technicians, researchers, privacy NGOs, consumer rights organizations, activists or lawyers) already exist. Effective enforcement can use these existing structures and support and coordinate whenever possible, while being able to supply the missing resources or take independent action when necessary.

**III. European Focus.** While there are some very important initiatives and enforcement actions in the EU and EEA member states, there is little coordination or pan-European enforcement. Key to overcoming this situation is close cooperation and participation of existing national privacy initiatives, tech experts and consumer protection organizations. Effective enforcement is based on strong information sharing and a detailed overview of European and global legal options to optimize each enforcement effort.

**IV. Global Impact.** The European Union is one of the largest markets in the world. Many companies have their worldwide headquarters in EU member state or substantial operations within EU territories. Consequently all major players are usually subject to EU law. The EU's right to privacy and data protection is a human right, applicable to any person (independent of its citizenship or residence) and applies to all companies under the EU's jurisdiction. In addition, IT products are usually produced for an international market and are interconnected. This means that enforcement within Europe can set standards that are likely to have a direct or at least indirect global effect far beyond the EU.

**V. Private Sector.** Mainly for legal reasons only the private sector currently allows for strategic, pan-European privacy enforcement. While civil law enforcement has become pan-European, administrative procedures remain national. At the same time there is considerable enforcement by NGOs or opposition groups in the government sector in many member states. Consequently the proposed organization will focus on the private sector only.

**VI. Stable Self-Funding.** The aim of the organization is to be self-funding after an initial set-up phase. A number of options should allow to cover all costs through the operations of the NGO, such as fees for enforcement or the organization of class-actions, as well as settlements and alike.
More traditional funding options, such as membership, training, conferences and (legal) publications are also widely available in the area of data protection and privacy law and practice.

# CHAPTER 2: EXAMPLES OF PRACTICAL APPROACHES

- Fact-Finding
- Legal Enforcement Options
- Enforcement Fund
- Campaigns & PR
- Cooperation

# 2.1. FACT-FINDING

In today's practice, one of the largest problems for the enforcement of privacy rights is the lack of knowledge about the inner working of software, digital products and the IT industry. It is therefore crucial for any effective enforcement to have a major focus on systematically establishing reliable facts on privacy violations and data processing patterns that can be used in a legal procedure. There are numerous options - including technical means - that NOYB can use to overcome this situation, for example:

**Cooperation with Other Institutions and Organizations.** There are numerous groups, institutions and organizations that are already researching, hacking and testing systems today. Through cooperation with other institutions (e.g. universities, researchers, privacy NGOs, hacker or consumer rights organizations), resources and knowledge can be shared and fact-finding can be outsourced to a large part.

**IT Community Outreach.** Many facts are already known, but not widely reported or not independently verified. Constant scanning of the IT, hacker, privacy and other communities and other relevant sources could massively aid independent establishment of facts. An active presence of NOYB within these communities will be crucial to be supplied with relevant facts. All facts generated externally must be reproduced or verified through internal testing before use in legal enforcement.

**Access Request Tool.** The right to access allows consumers to get a copy of their data and additional information about the use of such data. While most companies do not disclose information about illegal behavior, access requests often lead to interesting traces, or allow for a deeper understanding of the systems. Inconsistencies between the responses to an access request and other facts can hint at breaches of the law. An automated tool that allows consumers to request access and share the gathered information with the enforcement organization ("donate your data") could lead to additional information. Existing national efforts for systematic access requests should be utilized and combined with the option to mandate NOYB under Article 80(1) of GDPR.

**Systematic Testing.** IT systems are inherently opaque. The functioning of most systems is unclear from the outside ("black box"). Through systematic testing it is however possible to establish solid facts. Dependent on the product there are different options to for example intercept data traffic, analyze locally installed software or run tests on remote systems. Test users could be asked to "donate" their web traffic for analyzing patterns and privacy violations, data flows, data use and sources.

**Market Investigations.** In many cases, it may be possible to participate in the commercial sector (e.g. acquire personal data, software or hardware) to uncover facts. Similar to "mystery shopping" NOYB could set up companies that engage on the data market for research purposes. Such investigations might be helpful to understand data flows, use and sources.

**Complaint Tool for Consumers.** Consumers who experience (directly or by accident) the consequences of illegal data processing, can be an important source in uncovering misuse of personal data. A reporting tool operated by NOYB could collect and systematically register such information. Consumers who file reports with NOYB, can also be supported as complainants in legal proceeding. The organization can give legal counsel or support legal actions in relevant cases.

**User & Victim Database.** To be able to find users of certain services and possible plaintiffs and/or complainants, a database of users and/or victims from different countries could be extremely helpful. Users of the different tools, consumers that complain about certain services as well as supporters could submit their usage patterns to be contacted in the case of a violation. This would allow NOYB to find users in whose name legal actions can be taken in a favorable jurisdiction.

**Whistleblower Tools.** Within the legal limits a "whistleblowing tool" could allow the submission of relevant information and evidence anonymously. Such tools may be the key to acquiring insider information on illegal data processing operations.

**Privacy Bounty.** In addition to (or in combination with) other information gathering means, it may be possible to grant a reward for information that has led to concrete success in enforcement. Within legal and ethical limits, the possibility of a monetary reward might be an extra incentive to forward information to the enforcement organization.

**Review of Legal Cases.** Previous legal cases are usually a rich source of disclosed evidence and previous arguments. In many cases, previous arguments might contradict argument in the present cases. This can, for example, include criminal cases in which certain data was used to privacy cases where certain allegations were denied. Previous legal proceedings can also indicate compliance history.

**Costs.** Reasonable costs for fact-finding are recoverable as expenses in many civil procedures and therefore cost-neutral.

# 2.2. LEGAL ENFORCEMENT OPTIONS

Key for effective enforcement is the use of a combination of all available enforcement options (strategic litigation) and a combination of ideal jurisdictions (strategic choice of jurisdiction), dependent on each individual case to maximize the impact while minimizing enforcement costs. While each case need individual assessments, the current law and the upcoming GDPR allow for the following enforcement options, as examples:

**Written Warnings.** The laws and practices of many EU member states allow issuing "written warnings" to data controllers. Data controllers, particularly those with little awareness of the law, may be persuaded by informal actions, thereby avoiding legal procedures. The law of some member states allows for recovery of the costs of warnings from data controllers. Written warnings thereby limit costs for the enforcement actions or even make them cost neutral.

**Complaints Procedures at DPA.** Under Article 77 of the upcoming GDPR, all member states are required to offer a legal complaints procedure with their national Data Protection Authority (DPA). DPAs have the necessary powers to fully investigate data controllers, including disclosure of data structures, software or on premises investigations. This form of procedure may therefore produce evidence or facts that could otherwise not be gathered by a private actor. The GDPR also allows an NGO such as NOYB to be mandated by users and thereby represent them. In addition member states can allow NGOs to file complaints independent from a mandate. Complaints procedures are free, but at the same time do not allow compensation or financing of enforcement actions. Complaints are especially useful in cases with factual and legal uncertainties.

**Civil Law Suits.** Article 79 of the GDPR enshrines the right to civil law actions against any controller within the EU. While civil law suits can be more cost-intensive, they result in directly enforceable decisions.
In most European jurisdictions, costs are limited and are reimbursed if the case is won. A solid European fund for civil law litigation, combined with innovative tools like procedure financing or "after the event insurances", may help to overcome the (often trivial) financial limitations for civil law suits. Dependent on national legislation, the organization may be able to represent users, limiting the costs for lawyers or support lawyers when reviewing documents obtained during discovery.
The GDPR clarifies that users have the right to claim compensation for privacy violations in cases of material and immaterial damages as well as injunctive relief. Consequently the civil law enforcement of emotional damages and alike, can be used to finance enforcement actions. It is especially useful in cases with a strong factual and legal basis.

**Collective Enforcement under National Civil Law.** Some EU Member States allow different forms of collective redress mechanisms (such as "opt-in" and even "opt-out" group actions where a large number of plaintiffs are grouped into one civil procedure). This tool was for example used by "fbclaim.com" to gather more than 25,000 Facebook users from around the world, to file a group action against Facebook Ireland over the misuse of personal data.

**Collective Enforcement under the GDPR.** Article 80 of the upcoming GDPR grants users the right to mandate NGOs to represent them before a data protection authority or in court in individual cases. Article 80 can be used to form "group actions" or "collective complaints", if a large number of users are represented by NOYB ("mass mandate"). This option also allows to choose favorable jurisdictions.
Subject to national law, member states can also grant NGOs the right to file complaints or sue independent from a mandate by an individual data subject ("abstract lawsuit"). This option will not be available in Austria, but NOYB could set up a subsidiary in a member state that will allow abstract lawsuits.

**Collective Enforcement under Consumer Laws.** Directives 93/13/EC, 2005/29/EC, 2009/22/EC, and a combination thereof, allow legally recognized consumer rights organizations to file enforcement actions concerning, for example, unfair terms (including privacy policies) and unfair trade practices independent from individual claimants. Successful cases were filed, for example, by German and Austrian consumer groups. This form of "abstract" action is independent from individual consumers and actual harm.
A member state has to declare an NGO as a recognized consumer group – a status that is then valid throughout the entire EU. NOYB will prioritize cooperation with existing consumer rights organizations.
After the establishment of NOYB, it may be feasible to achieve the status of a consumer rights organization for NOYB itself. Dependent on the laws, it may be feasible to set up "sub-NGOs" in certain jurisdictions where it is relatively straightforward to achieve the status of a consumer rights organization.

**Funding of Collective Enforcement.** Collective actions can be funded by procedure financing companies, which fund all costs of the procedure in exchange for a certain percentage of the recovered damages. It may be possible for the organization to charge a certain fee for organizing a group action and thereby generate funding through group actions.

**Criminal Charges.** To a limited extent certain member states also have criminal sanctions for the violation of privacy rights (e.g. phone tapping, hacking, commercial violation of data protection rights) which can be applicable in individual cases. Subject to research of national laws, complaints for violations of criminal laws may also be an option. It has the benefit of substantial general deterrence and low costs, but is only available in limited circumstances and often subject to public enforcement.

**Constitutional Challenges.** In recent cases, constitutional challenges, challenges under the Charter of Fundamental Rights (CFR) or the European Convention of Human Rights (ECHR) were very successful and had the benefit of wide application on a very fundamental level. Increasingly commercial disputes also allow to raise constitutional issues - especially in the area of data protection and privacy.

# 2.3. GROUNDWORK FOR ENFORCEMENT

In order to ensure the ideal enforcement, NOYB shall engage in developing the basic knowledge that is necessary for strategic litigation in the privacy area. These tools lay the ground for informed and strategic enforcement actions, that utilize the enforcement possibilities of the common market. Such tools are, for example:

**Analysis of Legal Systems.** To effectively enforce privacy rights, it is important to research different national procedural and material law. Dossiers about all relevant subject matters (e.g. litigation options and remedies) can ensure that the most effective legal paths are taken. As most companies operate internationally, it is usually possible to choose the jurisdiction that is the most favorable. Dependent on the case this may also reach beyond European countries by, for example, using US procedures that are in some situations more favorable to plaintiffs. A combination of different legal systems can help to overcome national limitations.

**Case Law Database.** With the entry into force of the GDPR, court decisions in all 31 EU and EEA member states are relevant for the interpretation of the law. It is key for effective enforcement to have a good understanding of the case law in as many member states as possible. A database with relevant case law should be built in cooperation with national partners (such as universities, researchers or NGOs).

**Legal Network.** Most lawyers are currently conflicted and can therefore only represent commercial actors. It is therefore difficult to find lawyers and legal scholars who have expertise in the privacy and data protection field and are willing to take cases on behalf of consumers or privacy NGOs.
A network of pro-privacy and neutral experts and lawyers in the relevant jurisdictions has to be developed to allow members of the public - but also NOYB - to be properly represented throughout the European Union. In addition the publication of this list of lawyers could create at least a “niche market” for lawyers representing consumers and pro-privacy cases.

**Knowledge Management & Sharing.** All results from fact-finding activities must be organized and retained. User complaints must be tracked and organized. A systematic register of traces can ensure that NOYB does not lose track of issues that were uncovered but did not lead to any concrete action previously.
Currently limited sharing of information among NGOs, legal teams, researchers and investigators hinder proper enforcement, while data controllers usually have a full overview over all enforcement actions against them. As far as possible, gathered information should be published by NOYB or shared internally among NGOs through an online register/platform that allows an exchange of information with others.

# 2.4. EUROPEAN PRIVACY ENFORCEMENT FUND

**Individual Users.** In practice many individual users are not willing to file legal actions against obvious privacy violations, because of (often rather trivial) costs that could arise if a case is lost. This leads to almost no litigation in privacy cases, even if costs are low.
A number of consumer rights, fundamental rights or environmental groups have overcome this situation by setting up funds or schemes to support individuals who want to enforce their rights, but who do not want to take the financial risk of legal procedures.
An enforcement fund covers all costs if a case is lost and thereby allows individuals to have their rights enforced at no personal costs or financial risk. The actual costs and litigation strategy can be managed by choosing only promising or relevant cases on a European level. Funding would therefore need to be subject to a high chance of winning, the specific financial risk and the political relevance of each case.

**NGOs & Activists.** Equally, existing NGOs and activist groups could be enabled to bring cases through a centralized European enforcement fund that allows risk management on a European level. By pooling the financial risk and funding of cases, the financial burden could be limited for each individual case. Larger risks could be based on a combination of different risk management and financing tools.

**Cooperation.** Currently the “Digital Freedom Fund” is established in Europe, with a similar aim to support legal enforcement of digital rights, but with a wider scope that includes government interference with privacy rights. It seems possible to cooperate in overlapping enforcement areas. More detailed conversations on collaboration are already planned.


## EXISTING MEDIA TIES

*"We have developed a large international network of media ties during the europe-v-facebook.org' project. This includes about 300 specialized tech reporters on our media lists and countless personal ties throughout Europe and the world that have proven to be very effective. I am happy to introduce this network to NOYB."*

Max Schrems

# 2.5. CAMPAIGNS & PR

Active and strategic media relations are crucial as a deterrent to privacy violations and to ensure a broad impact of an enforcement organization. Combining established formats from privacy and consumer rights movements, with new options of the digital sphere will allow broader impacts of campaigns and a larger positive effect of enforcement actions.

**Coordination with Advocacy NGOs.** All PR activities with relevance in the policy debate should be coordinated with current efforts by policy NGOs. Having solid facts, practical cases and firsthand enforcement experience can be useful for existing NGOs that are working in the advocacy and policy field.

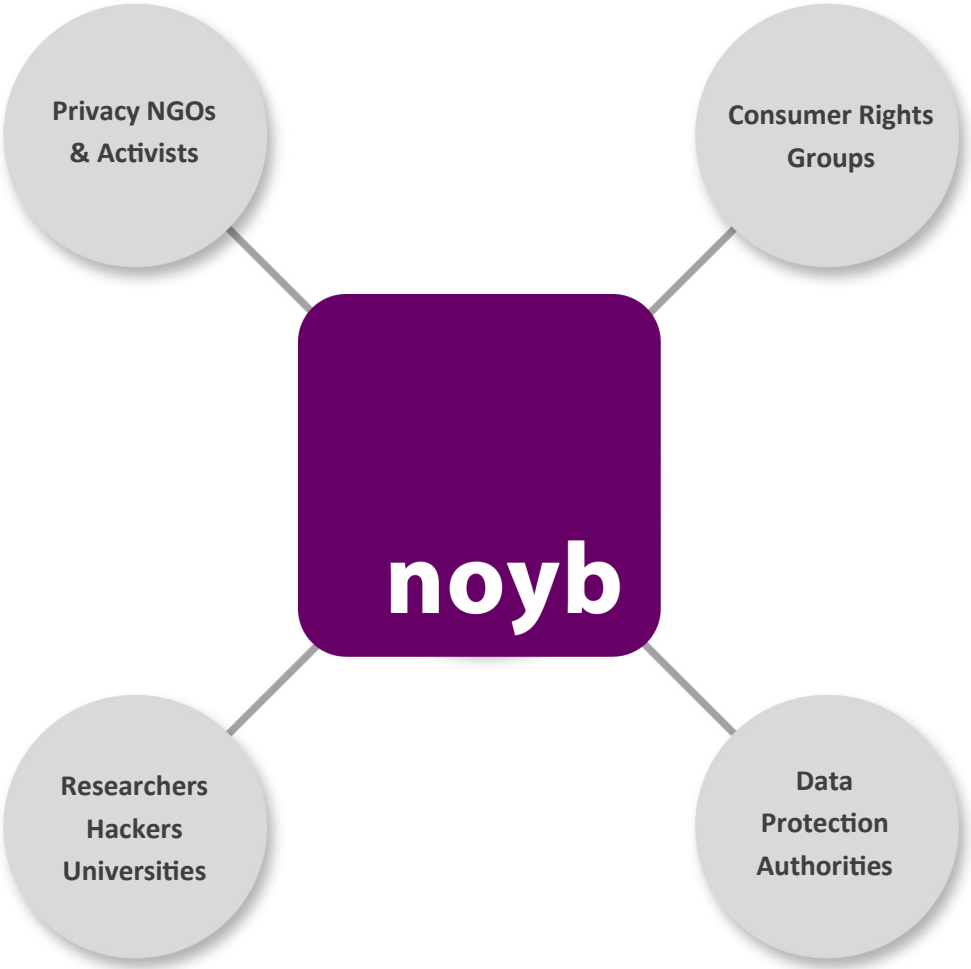
**Multilingual Information Portal.** The establishment of a multilingual central information portal is key to pan-European engagement. Information could include users' rights, uncovered facts, provide manuals for protecting users, lists of privacy-friendly alternatives for private and commercial actors or information about national data protection authorities. Content could be acquired and shared among partnering organizations, who often run well-made information pages themselves. Currently a large amount of information is not reaching the target audience due to language barriers. Content could be translated internally, by local partner NGOs and/or volunteers.

**Legal & Expert Newsletter.** Independent of the usual newsletters for NOYB members, a legal weekly or daily newsletter should allow to reach European privacy professionals with an academic, legal and European focus. This would help shift the current, rather industry-driven debate towards a more legal and academic debate, but also allow direct communication with the core privacy community.

**Statistics & Rankings.** Statistics and rankings allow the public to compare offers, put pressure on companies and stir public debate. Rankings and tests are commonly used by consumer rights organizations and have gained great importance in this field. Such rankings could also cover national laws and authorities (e.g. legal situation in the private sector, surveillance laws, resources and performance of DPAs). Statistical research may be done jointly with partners e.g. from the NGO or academic sector.

**Interactive Tools.** As many issues around data protection and privacy are very complex, the development of innovative tools could be helpful to increase awareness of facts and enforcement possibilities.
People may, for example, be more willing to exercise their right to access if there is a tool allowing them to make a proper access request under all jurisdictions and to a number of companies at the same time. Tools which visualize personal data use may help to generate awareness amongst people of all ages.

**Media Cooperation.** Key for a widely recognized organization will be extensive cooperation with international media. This may range from general press releases on current topics, cases and achievements, providing experts as interview partners, having joint projects with individual publications (e.g. conducting tests for the media or developing interactive tools), to specific campaigns. A large number of different formats of cooperation has already been developed in the consumer context and may be transferred to the privacy field.




## OPERATIONAL METHODS OF COOPERATION

Because of the wide variety of potential partners and the different possibilities and interests of these partners, the proposed organization should foresee a variety of methods of cooperation that fit different scenarios, including:

- Membership in the proposed organization by existing organizations
- Membership of the proposed organization in umbrella organizations
- Semi-formal cooperation (e.g. letter of intent or memoranda of understandings)
- Long-term joint projects
- Informal cooperation (e.g. project based or ad hoc collaboration)

# 2.6. COOPERATION

A defining feature of the existing European privacy NGO landscape is its fragmentation. Many NGOs cover only specific topics, or limit their work to specific member states. It is crucial for a lean and effective European privacy enforcement organization to cooperate with these existing consumer rights, privacy organizations from the start.

**Existing Privacy NGOs.** NOYB will not work on policy issues, user awareness or technical matters that are already well covered by other more experienced groups. Instead it will work to involve all relevant privacy NGOs and activists in the process of setting up a privacy *enforcement* NGO, with clear division of labor to avoid redundancy. Knowledge, networks and support can ensure that parallel developments are avoided and roles are defined properly. Wherever possible close ties should ensure trust between NGOs, permanent exchange of information and cooperation on common goals.
Depending on the developments, NOYB could also take over a coordinating role for European enforcement actions (e.g. coordinating legal challenges by different groups in different countries).

**Consumer Rights Groups.** Some consumer rights groups have also started to work on privacy related matters (e.g. the German VZBV or the Norwegian Consumer Council). However, it is usually not seen as a core competence and resources are limited. At the same time consumer rights groups are usually well connected, well-funded, influential and share similar objectives. Joint projects and enforcement actions could be beneficial for both sides (e.g. preparing cases and researching facts for consumer rights groups).

**Researchers.** There is a wide range of privacy, data protection and data security researchers, professors, activists or hackers with legal, technical or policy backgrounds. This existing knowledge should be utilized for NOYB through cooperation and joint research projects.

**Data Protection Authorities.** Some European DPAs are willing to actively enforce the law, but partly lack technical knowledge, evidence and facts. NOBY could supply these resources and trigger investigations.
DPAs may benefit from an exchange or the availability of research and information, which is made available to the public or submitted through legal procedures. Some DPAs stated that well-researched complaints may help them achieve their functions. A direct cooperation is however not foreseen as DPAs must maintain their status as neutral regulator.

**Hub Function.** An enforcement organization should also function as an information and cooperation hub for other groups in the field of privacy and consumer rights. A central archive, publications, exchange of information and coordination is vital to more coordinated and streamlined enforcement throughout the European Union.

# CHAPTER 3: GOVERNANCE

- Key Individuals
- Structure
- Location
- Staff

# 3.1. KEY INDIVIDUALS

The following individuals will ensure that NOYB has a broad basis in the privacy community and a stable governance structure that is independent from specific individuals.

**Managing Director**

*Mag. Maximilian Schrems**
*(*limited for start-up phase)*

appoints

**Executive Board**

*Mag. Maximilian Schrems*

*Ing. Mag. Dr. Christof Tschohl*

*Dr. Petra Leupold LL.M. (UCLA)*

elect

**Members**

# 3.2. STRUCTURE

Based on legal requirements and common practice in continental Europe, NOYB's articles of incorporation are based on a two-tier governance system. The current structure is following the requirements of the Austrian law on non-profit organizations ("*Vereinsgesetz*"). The governance system may be adapted to the size and structure of the organization in the future.

**Managing Director.** The managing director ("Geschäftsführer") is the full-time head of staff and is in charge of daily operations. He is appointed by and reports to the executive board and is vested with the rights to represent the organization. This function could be split into different responsibilities within a board of directors. For the start-up phase, this role will be exercised by Max Schrems on a *pro bono* basis. At a later stage this function should be transferred to a full-time employee.

**Executive Board.** The executive board ("Vorstand") is elected by the organization's members (general assembly) and consists of voluntary board members that meet on a regular basis (e.g. once a month).
It sets the long term goals and reviews the daily operations of the organization. It is the legal representative of the organization. The board should consist of persons in the field of IT, consumer rights and privacy law who are based in Vienna, to be available for board meetings in Vienna.
The initial board consists of Max Schrems (*lawyer, privacy expert - won e.g. C-362/14 on "Safe Harbor"*), Christof Tschohl (*lawyer, privacy expert - involved in e.g. C-594/12 on "data retention"*) and Petra Leupold (*lawyer, consumer rights expert, Austrian Consumer Rights Organization "VKI"*).

**Members.** Austrian NGOs need to be based by individual members, that form the general assembly. The general assembly of NOYB will consist of expert and institutional members and meet every two years.

- Institutional Members *(e.g. consumer rights institutions, privacy NGOs - with voting rights)*
- Selected Expert Members *(e.g. activists, key players, lawyers, tech experts - with voting rights*)

The general assembly should consist of about 20 to 40 members. This structure is intended to ensure stable and long-term operation, as well as inclusion of key players in the European privacy and digital rights community. New members are admitted by the executive board according to guidelines that ensure the necessary quality among the members and ensures a balanced general assembly.

**Supporting Members.** NOYB will also invite members of the public to become "supporting members", who will be a member of the organization, but do not hold voting rights in the general assembly.

**Other Functions.** There are additional functions required under Austrian law (such as a financial auditor and an internal arbitration mechanism), which are foreseen in the articles of incorporation. Additional functions, such as an "advisory board", can be introduced at a later stage.

# 3.3. LOCATION

**Legal Setting.** An enforcement organization should operate in a jurisdiction that is beneficial for privacy litigation. It should be generally pro consumer rights and fundamental rights, have a high degree of European integration, a track record of referring cases to the European Court of Justice and a high level of legal certainty. Limited legal costs, options like procedure financing and full reimbursement if cases are won are fundamental for cost-effective enforcement. On an organizational level it should be relatively straightforward to start and operate NGOs. It should be easy to cooperate with entities in other jurisdictions and to establish NGOs in other member states with favorable laws, if this turns out to be helpful. All of these elements are fulfilled in Austria.

**Political Situation.** Political independence from commercial interests in the IT sector seems vital for successful litigation. While there is a relevant IT industry, Austria has little to no economic footprint in the core business of commercializing personal data. Enforcement of privacy rights would therefore usually not trigger negative impacts on local business. Accordingly there is little political pressure against such an organization. On the contrary, Austria was so far a proponent of rather stringent rules. In practice this situation is highlighted by the intended financial and political support of the City of Vienna for NOYB.

**Economic / Practical Setting.** The organization should be located in a city that allows easy European and international cooperation and operation (e.g. spoken languages, travel options, existing NGO structures). An affordable, yet high standard of living will be crucial to attract possible employees at affordable costs. The availability of practical, political and financial support is equally relevant. Vienna fulfills these requirements.

Due to personal relationships and the considerations above, this proposal is based on **Vienna, Austria** as the main location for NOYB, where it was legally established in 06/2017.

# 3.4. STAFF

**Permanent Staff.** As a start, a minimum team of two legal and two technical experts should enable the organization to cover basic functions and allow continuity in both areas. An additional multilingual office manager will be necessary to take care of administrative matters. The position of a director could be initially shared by one of the experts. It is the aim to build a multinational and multilingual team from different parts of Europe to ensure a truly pan-European approach and through personal relationships. To ensure that NOYB is attractive for knowledgeable experts, the permanent staff should be financed on a long-term basis.

**Project Staff.** Additional personnel may be required for individual projects (e.g. experts with special technical skills) might be employed on a short-term ad hoc basis or contracted out.

**Additional Self-Financing Staff.** Dependent on the development in practice, it may be necessary and possible to add staff or interns for individual functions that are self-financing (like external projects or legal counsel of consumers).

**Internships / Volunteers.** In addition to the permanent and project staff NOYB may be able to attract interns and volunteers.

## INITIAL PERMANENT STAFF: ROLES

| | Tasks | Required Competences |
|---|---|---|
| **Director** (*) | • Management<br>• Representation | • Management experience<br>• Media experience |
| **Legal**<br>(senior & junior) | • Legal Fact-Finding<br>• Legal Research<br>Legal Community Outreach<br>• Preparation of Complaints and Lawsuits<br>• Legal Representation | • Strategic thinking<br>• Deep understanding of IT, privacy, consumer and EU law.<br>• Familiar with different legal systems<br>• Personal connections to relevant scene<br>• Basic technical understanding<br>• Multilingual (incl. English) |
| **Technical**<br>(senior & junior) | • Technical Fact-Finding<br>• Technical Research<br>Technical Community Outreach<br>• Development of Tools | • Background that allows strategic testing of different IT systems and reverse engineering<br>• Developer skills<br>• Personal connections in relevant scenes<br>• Multilingual (incl. English) |
| **Office** | • Office Work<br>• Accounting<br>• Consumer Outreach<br>• Minor Research Tasks<br>• Translations | • Perfect English and German skills<br>• Ideally fluent in other major European languages<br>• Basic Accounting skills<br>• Office experience |

** The function of the director should be performed by one member of the legal or technical staff.*

# CHAPTER 4: FINANCIAL ASPECTS

- Operating Costs
- Initial Costs
- Accountability & Transparency
- Initial Funding
- Long-Term Funding

# 4.1. OPERATING COSTS

***(THE PUBLIC VERSION CONTAINS LIMTED INFORMATIONIN ON THIS PAGE FOR STRATEGIC REASONS. THE FINANCIAL WORKINGS OF AN NGO CAN BE A CRUCIAL FACTOR IN STRATEGIC LITIGATION. WE HOPE YOU UNDERSTAND THIS DECISION. WE LIST ALL ELEMENTS OF OUR COSTS, BUT NOT THE DETAILED DISTRIBUTION ON EACH ELEMENT.)***

**Staff.** Calculations are based on a staff of five people (a senior and junior legal and technical expert and one office staff), based in Vienna, Austria.

**Office Space.** Office space for 5+ people (100 m², including fees, management costs, at mid-range locations in Vienna).

**Infrastructure.** Besides an office, the organization would need to have proper software, telecom and internet lines and IT equipment to undertake investigations and testing, as well as the networking and coordination functions. Overall it appears that the necessary infrastructure is standard and not particularly expensive.

**Projects.** A certain budget for smaller projects like cooperation with researchers, universities, NGOs, developers and other external partners should allow quick and straightforward implementation of such projects.

**Enforcement Fund.** The enforcement fund is a steady amount of money that secures chosen procedures. The risk taken should be based on a calculated amount of losses per month.
Large cases should also be based on “crowdfunding” or donations. These donations can be dedicated to the enforcement fund if a procedure is won and costs were recovered.

**Other Costs.** Other costs include funding for litigation, insurance, travel costs, legal literature, daily office expenses, possible membership fees of the proposed organization in umbrella organizations and alike.

Based on these estimates an initial annual draft budget of about € 500,000 appears to be realistic to perform the basic functions and tasks of the proposed organization.

***(THE PUBLIC VERSION CONTAINS LIMTED INFORMATIONIN ON THIS PAGE FOR STRATEGIC REASONS. THE FINANCIAL WORKINGS OF AN NGO CAN BE A CRUCIAL FACTOR IN STRATEGIC LITIGATION. WE HOPE YOU UNDERSTAND THIS DECISION. WE LIST ALL ELEMENTS OF OUR COSTS, BUT NOT THE DETAILED DISTRIBUTION ON EACH ELEMENT.)***

## 4.2. PROJECT PHASE COSTS

The initial project costs (press conferences, web page, promotion videos, "*kickstarter*" platform for memberships) would include the initial phase from November 2017 until the decision to become operational in Q1 2018 is taken.

## 4.3. INITIAL SET-UP COSTS

In addition to the operating costs a reasonable amount for initial costs (e.g. infrastructure, equipment, fees) must be expected. The initial target for an "enforcement fund" has to be raised.

## 4.4. FINANCIAL ACCOUNTABILITY & TRANSPARENCY

Under Austrian law NGOs may only use funds to pursue their non-profit aims and are bound by the relevant tax laws and the law on NGOs ("Vereinsgesetz"). The law requires an external auditor ("Rechnungsprüfer") who checks and verifies the financial dealings of the NGO.

Additional measures shall be taken, to ensure necessary transparency and a basic understanding of the sources and use of funds. Certain limitations may arise through legal requirements and the requirements of strategic litigation.

# 4.5. FUNDING OF OPERATIONAL COSTS

## I. INITIAL FUNDING DURING START-UP PHASE

The basic functions and the permanent staff of the organization must receive stable long-term funding. Concentrating on a number of large funding sources for the initial setup phase allows swift implementation of the organization.

**"Kickstarting" Supporting Members.** Given the wide network of existing supporters of Max Schrems and the existing media ties, NOYB will launch with a "*kickstarter-like*" campaign to generate a fixed number of supporting members. If the target of €250,000 is not reached within the relevant timeframe, the NGO will not come into existence. The known elements of crowdfunding campaigns (e.g. limited time, domino effects) should be used to attract supporting members instead of the usual one-time support on crowdfunding systems. Individual supporting members that match a certain amount per year should be granted benefits (e.g. free legal counsel) to make long-term membership of a certain amount attractive. Based on this foundation of supporting members, NOYB should develop classical memberships further.

**Institutional Funding / Major Donations.** As far as possible the remaining operating costs of € 500.000 for at least three to five years should be backed by institutional funding (foundations, pro-privacy businesses, public funding) and long-term individual memberships and donations. The key objective is a mix of funding sources, to ensure factual independence of NOYB (multi-pillar system).

**Contributions in kind.** Office space, hardware, software, legal literature, legal databases or IT services could be provided by partners and supporters as contributions in kind. An existing network of personal ties should be used to mitigate expenses for office space, infrastructure costs and alike considerably.

## II. ADDITIONAL LONG-TERM FUNDING OPTIONS

After securing funding for an initial start-up phase of 3 to 5 years, the following options should be used to diversify funding and become self-funding after the initial start-up phase.

**Public Funding.** It may be possible for the organization to receive public funding. However the fact that the organization will operate on a European level may be an obstacle to national funding while European funding is traditionally hard to secure on a long-term basis.

**Project-based Donations.** A high level of visibility can lead to substantial donations. In recent times concrete "project based" donations (similar to "crowd funding") appear to be more likely than long-term institutional funding. Especially high profile cases, like the challenge to "Safe Harbor", received substantial donations that enabled the bringing of a large case without financial risks, and even resulted in a surplus of more than € 50.000, when the case was won.

**Enforcement Actions.** Funding through enforcement can in main cases combine the aim of NOYB (enforcement) with the funding of this aim. The following options are for example available to self-fund enforcement actions, or even contribute to the general budget:

- **Legal Counsel:** While general information should be provided for free, detailed legal counsel and representation before courts and authorities could be offered at a reasonable fee.
- **Written Warnings:** In certain jurisdictions, it is possible to charge a fee for a "written warning" sent to a company engaging in unfair trade practices. While this form of funding is limited to certain jurisdiction, it could help to self-fund enforcement costs, when used in a wise and modest form.
- **Group Actions:** Collective Actions can be organized for a fee (e.g. a small percentage of the successful claim will be donated to NOYB for administration). As privacy violations are usually uniform and there is a large number of victims, these cases can theoretically reach substantial amounts (e.g. € 1 billion, if 1 million users have a claim of € 1000 as compensation), even just small administration fees, can therefore provide substantial funding.
- **Settlements:** Especially large cases are often settled. Part of the settlement could be donations to NOYB.
- **Procedure Financing:** Procedure financing companies can take the financial risk of a case for a certain percentage if a case is won. This could ensure that lost cases do not lead to negative financial consequences.
- **Loser Pays:** Most costs for litigation can usually be claimed from the other side when a case is won. As NOYB can pick its battles and would primarily focus on the most extreme violations of the law, it is likely to win a substantial part of cases and reclaim the costs of enforcement.

In summary, these and other options may enable NOYB to become predominantly self-funding when enforcing users' right to privacy in the long run. Naturally these options have to be used with prudence.

**Outreach & Sales.** Other NGOs have made considerable profit through the sales of publications, education programs or specialized conferences, and even merchandise.
Especially through the coming into force of GDPR a considerable need for education, conferences and schooling can be observed. Legal and technical publications and schooling is usually well-paid. NOYB could combine outreach and funding in this profitable area.

**For-Profit Privacy Services and Products.** Finally NOYB could get active in "for profit" areas, that also further the aim of ensuring that the right to privacy is observed in practice, for example:

- GDPR foresees certifications and seals to demonstrate compliance, which could be managed by NOYB.
- GDPR requires data protection officers in many businesses. Professional training could be offered by NOYB.
- Equally NOYB could engage in the development and distribution of privacy friendly alternatives (e.g. software).

From a credibility standpoint such engagement must ensure that the organization provides a 'gold standard' and conflicts of interest are avoided. It may be preferable to outsource such activities to an independent and separated subsidiary of NOYB (e.g. a separate for-profit company, owned by NOYB).

## 4.6. FUNDING OF INITIAL COSTS

It is to be expected that a certain amount of potential donors in a "*kickstart*" campaign of supporting members, will not be willing to donate on a long-term basis. **€ 100,000** should be crowdfunded through such donors. About **€ 50,000** of the € 150,000 of initial costs and additional **€ 10,000** for the NOYB project phase will be provided by "europe-v-facebook.org".

# CHAPTER 5: TIMELINE & FIRST PROJECTS

# 5.1 POTENTIAL FIRST PROJECTS

*The following list represents an initial list of wider potential first projects. A final list of concrete enforcement actions should be developed after the establishment of NOYB and cannot be published for strategic reasons.*

**TECHNICAL: Testing Environment for Apps.** As an initial technical research project the organization could review the actual data use by the most popular smartphone apps and thereby develop a testing environment for consistent testing of apps. Existing research have e.g. shown that some apps access GPS locations or contacts beyond what is strictly necessary for the function used. The generated evidence could lead to rankings, complaints or legal procedures.

**LEGAL: Smartphone Operating Systems.** Apple and Google dominate the smartphone market. Their policies are based on a "take it or leave it" basis and allow these companies significant access to the most personal device of most consumers. Enforcement actions in this area could have a substantial impact in the daily life of almost every citizen.

**RESEARCH: Laws and Enforcement Options.** An initial legal research project could be a detailed review of the member states' laws on consumer protection, privacy and data protection laws, as well as the current case law and enforcement options and costs. This project could feed into the "enforcement tools" described in this proposal.

**ADMINISTRATIVE: Mapping the playing field.** An overview of major players in the tech industry is crucial for legal enforcement. A review of the company structures, legal procedures they were involved in and other resources allows to find the preferred jurisdiction. At the same time a review of all national DPAs and national procedures should allow to identify preferred DPAs to file complaints and cases.

# 5.2. AIMS BY THE END OF 2018

- Cooperation with at least five major privacy NGOs, five consumer rights organizations, five universities or research institutions and five hacker institutions/spaces.
- Basic network of lawyers at least in Austria, Germany, Ireland, Luxembourg and the US.
- Support of 10 small external enforcement actions through the enforcement fund.

# 5.3. TIMELINE

**End of Q3 2017 | Preparatory Phase**

- Legal registration of organization
- Initial preparations, finalization of concept papers
- Recruitment of initial board members and initial voting members of the organization
- Seed funding by "europe-v-facebook.org" (€ 60,000) for project phase

**During Q4 2017 | Kick Off Phase**

- Finalization of promotion material and website for "kick off" phase
- Public launch of the NOYB project proposal
- Campaign to "kickstart" supporting members

**Beginning of Q1 2018 | Decision: *Go!* or *Stop!***

- Final list of contributions in kind
- Final list of supporters and potential cooperating partners
- Clarification of the availability of funding for an initial 5 year period

**End of Q1 2018 | Start of Operations**

- Operational start (set-up of office spaces, basic infrastructure, webpage and alike)
- Hiring of initial permanent staff
- Set-up of initial network and agreement on initial project schedule (see left)

**During Q2 2018 | First Enforcement Actions**

- Coming into force of GDPR on May 25th
- First enforcement actions under GDPR on May 25th

**End of Q4 2018 | Full Development of NOYB**

- Set-up of complaint and whistleblower tool
- Set-up of centralized knowledge management & sharing system
- Initial outreach schedule (meetings, speeches, conferences)
- First "privacy ranking" published
- First systematic testing schemes
- Set-up of access request tool

**Mid-Term Growth**

After an initial set-up of the core operations in 2018, NOYB should continuously grow and work on enforcement actions. Volunteers, staff and funding should be stabilized and grown in line with enforcement actions. First external funding sources (e.g. trainings, publications) should be developed.

**Long-Term Growth**

Depending on the experience, further expansion or diversification may be desirable. It may, for example, be realistic to widen the scope of the organization from privacy to other digital rights (e.g. net neutrality) or related consumer rights (e.g. unfair terms) or to set up national NGOs in countries that currently lack local initiatives.

**Impressum:**

Verein NOYB
Annagasse 8/8
1010 Vienna
AUSTRIA

www.noyb.eu
info@noyb.eu

ZVR-Nummer: 1354838270