OPEN SOCIETY
FOUNDATIONS

Civil Society Organizations and General Data Protection Regulation Compliance

Challenges, Opportunities, and Best Practices

ABOUT THE ORGANIZATIONS

The Open Society Foundations, founded by George Soros, are the world's largest private funder of independent groups working for justice, democratic governance, and human rights. Open Society funded this report hoping to make a contribution towards stronger data governance in civil society.

Data Protection Support & Management is a niche data protection consultancy specializing in assisting humanitarian organizations, nonprofits, research institutes, and organizations dealing with vulnerable data subjects and complex processing environments These efforts aim to help these groups and organizations innovate responsibly and comply with their data protection obligations.

ABOUT THE AUTHORS

Vera Franz is deputy director of the Open Society Information Program where she oversees the global portfolios responding to threats to open society created by information technology. For the past decade, Franz has worked to develop and implement field strategies to confront corporate data exploitation and government surveillance. This work has included supporting the adoption of a robust EU General Data Protection Regulation (GDPR), and initiating the Digital Freedom Fund, Europe's first digital rights litigation fund. She is a certified data protection officer and a member of Open Society's GDPR compliance group. Before joining Open Society, Franz was a researcher at the Techno-Z Centre for Innovation & Technology and taught at the Department of Communication Studies at Salzburg University.

Ben Hayes is a director of Digital Protection Support & Management. Hayes previously worked for NGOs and research institutes on issues related to national security, border control, counter-terrorism, policing, criminal law, and human rights. Before co-founding Digital Protection Support & Management, Hayes worked as data protection legal advisor to the International Committee of the Red Cross and as a data protection expert for the United Nations Refugee Agency. He has also consulted extensively on applied "data ethics" issues for the European Commission's Directorate General for Research and Innovation and the European Research Council.

Lucy Hannah is a data protection consultant with Digital Protection Support & Management, a certified data protection officer, and an Australian-qualified lawyer, working across Europe and the United Kingdom. Hannah has extensive experience in privacy, data protection, and regulatory compliance. She previously worked on GDPR compliance for an international publishing organization in London and for a UK-based online retailer, overseeing the technical and operational changes needed to meet the businesses' data protection compliance requirements.

1. Introduction

As civil society organizations are becoming increasingly data-heavy operations, basic fluency in data protection is essential. Adapting to the changes brought by the EU General Data Protection Regulation (GDPR) will make civil society organizations more resilient and enable them to appropriately protect the personal data of their staff, donors, beneficiaries, research subjects, and contributors. In an era in which the political and operational space of civil society is "shrinking," compliance with the GDPR also provides a robust defense against adversaries who may seek to use or abuse the GDPR in an attempt to undermine the activities of these organizations. Fluency in data protection also allows civil society organizations to lead by example on the value of data privacy and demonstrate an alternative to the current model of unchecked, large-scale data exploitation by many big technology companies.

We were motivated to produce this report as we witnessed many NGOs (non-governmental organizations) tie themselves up in knots over their mailing lists in the run up to the GDPR. Countless civil society organizations flooded our inboxes with needless re-consent requests, while large corporations gave the impression of business as usual. With this report, we set out to better understand what the GDPR means for NGOs in very practical terms, and provide some practical guidance to NGOs on issues that they have struggled with.

We wanted to understand NGOs' attitudes toward the GDPR, the guidance on compliance available to them, the particular compliance challenges they encountered, and the impact the GDPR has on their core activities such as advocacy and human rights investigations. For example, is the approach to mailing lists, where many NGOs unnecessarily culled the addresses of recipients, characteristic of the non-profit compliance experience as a whole? Conversely, is the NGO sector under-complying as it is overly-reliant on the premise that its activities are all in the "public interest" and therefore a priori permissible under the GDPR? Also, we were particularly interested in exploring whether and how the GDPR has been or may be used by political opponents against civil society organizations and how the GDPR fits in with the growing compliance burden associated with the shrinking space for civic activism on political issues. There can be no doubt that tenacious civil society organizations have made powerful enemies; does the GDPR therefore leave them exposed to legal action by vexatious and litigious adversaries? Are they aware of these risks and have they taken adequate steps to mitigate them?

The authors firmly believe in the importance of comprehensive data protection, and the GDPR more specifically. Despite its detractors, the GDPR is without doubt the best entry point to begin to address the damage that massive data exploitation by big tech companies is doing to our societies—from political microtargeting and societal polarization to the out-of-control "ad tech" industry and the emergence and consolidation of tech monopolies. But we also acknowledge the challenges the GDPR creates for civil society. For example, while smaller organizations are exempt from certain compliance requirements such as the appointment of a data protection officer, most of the legislation applies in its entirety regardless of organization size and the compliance burden can disproportionately impact these organizations. This was recognized by the European Commission, which established a dedicated budget-line to help national data protection authorities assist small and medium-sized enterprises in understanding and complying with the GDPR.[1] This was aimed squarely at businesses, with no provision for the hundreds of thousands of non-profit organizations across Europe.[2] It is also notable that whereas most business sectors lobbied for exemptions, special treatment or lower standards in the GDPR to protect their commercial interests and activities, civil society organizations generally lobbied for high standards across the board—without necessarily thinking about the implications for their own work. So while media organizations had sought to ensure that the GDPR did not unduly restrict press freedom, other public interest organizations were not so forward-thinking, which appears to have left a few "gray" areas.

We hope this report can provide some practical guidance to NGOs on issues that they have struggled with: not by producing yet another GDPR checklist or "compliance tool," but by thinking through the compliance issues that may be unique to civil society organizations engaged in social justice and human rights activism. Unfortunately, there is no getting away from the complexity of the GDPR—a problem compounded by the freedom left to the member states to apply and interpret many of its key provisions in accordance with their own national legal traditions—so the usual caveat about making additional checks for consistency with national law before relying on anything in the best practice section at Annex 1 applies.

The structure of the report reflects the challenges and opportunities that our work revealed. In section 2, we discuss in more detail our findings from the survey and the follow-up conversations we engaged in. The following

1 "Restricted call for proposals: Ensure the highest level of protection of privacy and personal data," *Funding and Tender Opportunities*, European Commission, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017, March 30, 2017.

2 In 2015, data compiled by the Donors and Foundations Networks in Europe and the European Foundation Centre and analyzed by the Foundation Center (New York) suggested that there are more than 141,000 registered "public benefit foundations" in Europe. Because many civil society organizations are unregistered, their total number is likely to be much higher, *Number of Registered Public Benefit Foundations in Europe Exceeds 141,000*, Lawrence T. McGill, Foundation Centre, available at https://www.swissfoundations.ch/sites/default/files/European_Foundation_Sector_Report_2015_0.pdf, 2015.

sections cover notable issues that arose as the project went on. Section 3 provides two examples of when civil society organizations have been sanctioned for non-compliance with data protection law, and the lessons that can be learned by other civil society organizations. Section 4 looks at the way in which Subject Access Requests—which are derived from the fundamental right to access data about us collected by governments and businesses—have been used positively by civil society organizations, but also at how organizations have received and handled frustrating and unfounded requests. Section 5 explores the difficulty of disentangling data protection from wider societal issues of power and resistance, and considers its impact in terms of both push back against civil society organizations, and as a key factor in establishing an "enabling environment" that civil society needs to achieve positive social change. Sections 6 and 7 attempt to draw together the conclusions of our findings and make recommendations for different stakeholders. Annex 1 provides best practice guidance for civil society organizations based upon our research and wider experience of dealing with GDPR compliance.

2. Our Research Findings

While the GDPR addresses some fresh issues and did introduce new safeguards and restrictions on data processing, it is worth pointing out that most obligations pre-dated the new legislation. Many core principles and requirements in national and European data protection law have been present for almost 40 years.[3] Yet there was certainly no shortage of hype and fear mongering around the introduction of GDPR—much of it linked to consultancy sales pitches. In the following, we summarize how NGOs have responded to the GDPR.

2.1 High-level Findings

Mixed attitudes toward GDPR compliance: Many respondents emphasized that GDPR compliance is in line with organizational values, but many also pointed out that compliance is challenging for a whole set of reasons, not least because it is time and resource intensive. There is broad agreement that the application deadline for the GDPR represented an opportunity to review organizational data practices, but some respondents also stated that when added to a growing compliance burden already encompassing a raft of NGO transparency and accountability requirements, GDPR regulations make it harder for civil society organizations to concentrate on their core activities.

3 See EU Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981).

Lack of good GDPR compliance advice, especially advice tailored to non-profits: This is what we found in our literature review of available guidance, and it was also emphasized by many survey respondents. Official advice from data protection authorities seems to be particularly lacking in Eastern Europe, while the British, Dutch, and French authorities were singled out for providing the most useful advice, even though much data protection advice is rarely tailored specifically to non-profits. Where relevant guidance does exist, it is aimed at charities, and while some non-profits are charities, their activities, particularly their activism, tend to raise a different set of issues. The guidance for the charity sector is in turn dominated by the issue of fundraising, where best practice documents and detailed guidance are available. The provision of substantial information about fundraising is in response to fines recently issued by regulators against international NGOs and others for their aggressive fund-raising tactics and failure to protect donor data.

Reliance on external, tailored commercial advice: Many of the respondents also pointed out that they were largely beholden to the commercial compliance industry that was so visible in the run-up to May 2018, offering packaged solutions often for a significant fee. The complexity of the law, a lack of internal capacity, the need for clear guidance, and the various risk appetites of civil society organizations all contributed to why many respondents said they had to seek advice from external lawyers or consultants. The majority of respondents (75 percent) indicated they were satisfied with the guidance they sought in navigating the uncertainty and lack of clarity around their GDPR obligations. The remaining 25 percent—a significant proportion of respondents—indicated that the commercial advice received was conservative or otherwise unhelpful. This phenomenon could be partially responsible for instances of NGO over-compliance.

Expenditure of time and money on compliance: Two thirds of NGOs started their compliance efforts in early 2018 or later, the rest started earlier. The majority of survey respondents (75 percent) paid for advice from consultants and/or lawyers. Not surprisingly, the larger the organization, the more time and money was spent on compliance.[4] The exception to this rule is a very small organization, which spent 40,000 euros (a third of their annual organizational budget) following a data breach and an investigation by the Data Protection Authority. For half of the groups, the cost of compliance was negligible, but almost a third indicated that they spent up to 10,000 euros . The three that spent more than 50,000 euros

4 Forty percent of survey respondents spent less than one month on compliance—most of those were small NGOs with 1 to10 employees. Only four respondents, large organizations, spent more than one year on compliance.

have annual budgets of over 1 million euros . Some survey respondents also reported plans to upgrade their IT infrastructure to ensure better compliance with the GDPR, including migrating data into new systems with granular access controls. These upgrades would require major financial investments. This matters because financial resources are often scarce and larger NGOs are under pressure to minimize overheads relative to the money they spend on programmatic work.

Evidence of over-compliance: The most widespread example of over-compliance was the decision by many NGOs, often on the basis of external legal advice, to ask all of their mailing list subscribers to "re-consent" to receiving newsletters and other organizational communications. The results of this for many NGOs was that the number of mailing list subscribers was slashed, in some instances, quite dramatically. Less worried and arguably better-advised non-profits instead simply acknowledged the entry into force of the GDPR and/or updated their privacy policies, stated that they believed subscribers wished to continue receiving their communications and provided them with the opportunity to opt-out at any time. Beyond this issue, concerns about over-compliance were widely shared among respondents. Another NGO, following the advice of their external data protection officer, undertook a data protection impact assessment of all their data processing activities. While impact assessments are the best practice, the NGO that underwent the assessment holds very limited personal data and undertakes no marketing or outreach activities. It certainly did not meet the legal threshold for a mandatory impact assessment.

Examples of a pragmatic compliance approach: Several NGOs acknowledged the requirements of the law, but chose to take a risk-based and proportionate approach, in some cases against external legal advice. For example, one international NGO was (wrongly) advised that they should nominate a data protection officer in every EU jurisdiction, but decided to ignore this advice because of the exorbitant cost involved. Instead, they contracted a single, external officer instead. Another organization decided not to seek consent for the use of contact details for communication with public officials, even though external counsel had advised the opposite. Had the organization followed this unfounded advice, then its ability to communicate with policy makers—a core part of its mission—would have been seriously restricted.

2.2 Specific Compliance Challenges

Civil society groups' attitudes toward compliance are likely shaped by the concrete experiences they have had working to achieve compliance. We asked organizations that had struggled to comply what issues have been the most difficult and why.

One of the biggest challenges identified by NGOs is the identification of the correct legal basis for their data processing operations: Although it is often assumed that the GDPR is all about obtaining consent from the data subject, consent is merely one of six "legal bases" for processing, and by no means the most widely used. From the feedback we received, it seems NGOs found it easier to define the legal basis for their operational and administrative work, but several NGOs are still uncertain about the legal basis for their programmatic work. "We have all our non-programmatic processing documented. Employees, donors, etc..." said one NGO worker. "I am comfortable with the legal bases. But I have questions about our journalistic activities. We have an internal memo that says we take a wait and see approach. If we don't get hit by regulators, over time everything will become a lot clearer." It also appears that many of the NGOs we spoke to are relying on the "public interest" legal basis in the GDPR for their research and investigative activities, as well as exemptions designed for media organizations. However, the extent to which NGOs can rely on journalistic exemption when they provide research support services to investigative journalists is far from clear. The relevant exemption provisions are subject to national interpretation, which means that what is permissible in one member state may not be permissible in another. Moreover, to date only 18 member states have notified the European Commission about how they are implementing the GDPR provisions relating to freedom of expression and information. Even transnational organizations seeking legal certainty cannot yet find it. The European Data Protection Board, which promotes cooperation between national data protection authorities and contributes to the consistent application of data protection rules in the European Union, has recognized these challenges and plans to issue guidance on the balance between free expression and data protection.

The development of a data retention policy was another widely quoted compliance challenge: Such policies are required because under the GDPR, organizations need to adhere to the data minimization principle. This principle stipulates that the amount of personal data and the length of time for which it is stored must be limited to what is necessary for the purposes for which it is processed. The particular challenges highlighted by NGOs are the definition of retention periods (How long can the data be kept? How is necessity determined?) and the institution of access controls (Who can have access to the data?). One respondent highlighted the financial burden of implementing such a policy: "People should only have access to data they need. Right now, a lot of people have access to everything. Our systems are not made in this way yet. We are only contemplating this [moving data over to a new system with appropriate access controls] because of the GDPR. This is cost-intensive." Another

respondent identified challenges around the technical limits of third-party platforms and tools used to process personal data, i.e., some tools make it very difficult to permanently erase data: "For example, when testing one tool—it only allowed us to delete profile information about a subject, but not discussions the subject had posted! We're still working on how to ensure we can comply with all subject access requests when using third party tools."

Several NGOs shared concerns about data security: One particular security concern for a number of NGOS was the risk of data breaches as a result of malicious attacks. The GDPR requires all data controllers to take a risk-based approach and enact technical and organizational measures commensurate to the threats they face and the risk that unauthorized access or disclosure of personal information poses to data subjects. This is something that small NGOs in particular are not very well placed to achieve, as noted by survey respondents. "The level of resources and expertise available to NGOs is no match for sophisticated, targeted attacks," said one respondent. This is an area where non-compliance with the GDPR can become a big vulnerability for NGOs. In the event of a breach, the technical and organizational measures that have (or have not) been introduced by an organization will be key in determining culpability. Preventing breaches requires demonstrable efforts to enhance information security and documentation of compliance efforts, which is particularly challenging for small organizations.

Operating across multiple jurisdictions: A number of groups said they faced significant challenges in meeting privacy rights requirements that could vary throughout Europe. Derogations for freedom of expression, research, and archiving are some examples of a whole host of areas in which member states can deviate from and surpass the minimum requirements laid out in the GDPR when implementing national law. "We struggled with conflicting interpretation of certain provisions between jurisdictions," said one group member. Another one commented: "We can't rely on advice from individual data protection agencies (DPAs) for all European jurisdictions we operate in." A member of another group that works in a decentralized and remote way remarked, "We weren't sure which national regulatory authority to consult, as we all live in different countries."

The GDPR requires data controllers to concern themselves with the terms and conditions of agreements with third party processors: A major challenge this presents is the fact that not all third party processors comply with the GDPR (at the time of writing even software and licensing agreements provided by large companies like Microsoft are under investigation for non-compliance in key areas).[5] The power imbalance between NGOs and large processors is stark, giving NGOs little to no influence over the content of agreements made with third parties. "The GDPR made us take a serious look at the terms and conditions of the tools that we had signed up to," said the director of an NGO. "Some were great, clearly noting that they were GDPR compliant and having simple to understand terms, which backed up their claims. Others were not so great. Clearly, some providers still need to make changes for the GDPR." To ensure third parties' compliance status, a review of both terms and conditions and the functionality of putting these into practice is required. As NGOs and organizations in other sectors start to prioritize GDPR compliant processors, it is hoped that processors will start competing on grounds of privacy and data security status.

Reconciling the GDPR with the ePrivacy Regulation: Discrepancies between the GDPR and the ePrivacy Regulation was an area of concern for a number of survey respondents. The ePrivacy Regulation,[6] last updated 10 years ago, addresses e-marketing, privacy of communications content, and metadata as well as cookies, while the GDPR regulates personal data protection more broadly. A new and updated ePrivacy Regulation was intended to be released at the same time as the GDPR, but heavy lobbying from companies in the adtech and online publishing ecosystem continues to delay its finalization. As a result, there is tension between the laws as they currently stand; in practice this is primarily around the issue of "consent" in the context of cookies.[7]

The online publishing industry in particular has responded with outcry over the current practice across Europe of presenting cookie banners. The banners tell a device user that a website places cookies and implies that the user is giving consent if they continue to navigate the website. Current banner practices could be reconciled with the much higher threshold of explicit, unambiguous, and revocable consent as set out in the GDPR. Across the internet, this issue has confused website owners, with even the United Kingdom's Information Commissioner's Office admitting its cookie consent process was incorrect in June 2019.[8] An array of approaches have been taken to managing

5 "EU Data Regulator Launches GDPR Probe into Microsoft Software Deals," Graeme Burton, *The Inquirer*, https://www.theinquirer.net/inquirer/news/3073900/eu-gdpr-probe-microsoft-software-cloud-contracts, April 9, 2019.

6 Directive 2002/58/EC of the Euopean Parliament and of the Council of Europe,July 12, 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

7 *The Urgent Case for a New ePrivacy Law*, Giovanni Buttarelli, European Data Protection Supervisor, https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en, October 19, 2018.

8 Twitter update from Adam Rose, https://twitter.com/adam_rose/status/1140151337834962944?s=21, June 15, 2019, although the Information Commissioner's Office's cookie notice has been updated since this time.

cookie consent and at present many websites offer data subjects granular control over the cookies dropped on their devices prior to landing on a webpage through the use of off the shelf "consent management platforms." These platforms can be configured to offer website visitors the opportunity to opt-in to the use of non-essential cookies, for advertising or third party tracking etc. This meets the GDPR standard for consent.

Primarily, this is an issue that will affect media and publishing organizations dependent on cookies to track their readership in order to drive advertising revenue. While it does not directly touch upon the programmatic work of civil society organizations, it is something that every organization with a website must be aware of while remaining alert to the changes that the impending ePrivacy Regulation may bring.

2.3 Impact of Compliance Efforts on Core Activities

The GDPR has not had a major impact on NGO core activities such as advocacy and investigations: With the exception of the hysteria around mailing list consents and widespread enforcement action against charities in the United Kingdom over their aggressive fundraising practices, our survey found few other major GDPR impacts on programmatic work. However, the GDPR has only been in force for one year. Complaints by data subjects, enforcement actions by regulators, guidance from the European Data Protection Board, and interpretation of issues that overlap with other areas of legislation or are unclear, could all have an impact. It is also noteworthy that a small number of NGOs, given the uncertainties of the GDPR, decided to take a wait-and-see approach toward compliance of their core activities. One respondent argued that the public interest protections will apply and the organization would not invest in compliance in any major way at this point. These issues are considered in more detail below.

ADVOCACY

For the large majority of NGOs we consulted, advocacy is their core business. In this report, advocacy is understood as outreach not only to policymakers but also the public writ large. As noted above, around May 2018, many NGOs sent out messages requiring their entire mailing lists to "re-consent." The impact of this decision was drastic: "So far, the most evident impact [of compliance] on the organization was the drastic downsizing of the number of recipients of our mailing list(s) (from about 1000 to 104 contacts)." Another organization noted, "The main negative effect has been stripping back our number of email recipients list by 66 percent, from 45,000 people to 13,000 people. This has meant we have a smaller pool of people for marketing our ideas and fundraising."

There is now awareness among many NGOs that the decision to ask mailing list subscribers to re-consent was not necessary. An NGO representative said, "Our head of admin decided 2-3 days before GDPR came into force to ask everyone to re-consent. We lost 15,000 [a quarter] of our subscribers. And later we realized that we could have used legitimate interest as a basis for processing." Another remarked, "A rigid adherence to the rules has impacted on circulation lists for newsletters etc." One respondent identified that the climate of fear and uncertainty in the lead up to the GDPR coming into force, along with both a lack of technical capacity and the desire to take visible action toward compliance, may have contributed to many NGOs' decisions to radically cut their mailing lists.

Interestingly, not all see the slashing of mailing lists as negative. Some respondents feel that outreach has now become more focused with better response rates. One NGO representative, for example, said, "Our mailing list has decreased significantly because we deleted all the contact information on people we could not prove gave consent. Therefore, we increased our efforts to legally grow the database. However, the current mailing list has a much better response rate." Another respondent noted, "It [outreach] has become much more focused instead of random 'spraying' of advertisements."

Surprisingly, none of the NGOs seem to distinguish between public officials and non-public officials, except for this respondent: "Where it could have impacted our work, e.g., advocacy efforts that rely on database contacts, we have taken a pragmatic view toward compliance to try and ensure that we can continue to contact government officials about policy positions and events we organize, even though they may not have consented."

INVESTIGATION AND RESEARCH

Investigation and research into human rights abuses is another core activity of civil society. It fuels advocacy for social change in exposing abuses of power and fundamental rights, and is used to prosecute abusers, defend victims, and challenge oppressive laws.

This work is generally carried out by three types of groups: specialized investigative reporting outlets; human rights and social justice groups that combine investigation with campaigning and advocacy; and groups that support investigative journalists, human rights researchers, litigators, and advocates through the creation of data repositories and analysis. The latter category focuses on investigation and data gathering, but do not publish or advocate for change. This is relevant as national implementing legislation in some member states only makes provision for journalistic exemptions to apply to the processing activities of entities that "intend to publish" the results of investigations,

while the research and archiving exemptions have been designed with academic institutions and public bodies in mind. These issues—and how NGOs can deal with them—are considered in the best practice section at Annex 1 in this report.

FUND RAISING

While many of our respondents are smaller NGOs that tend to receive a substantial amount of support from institutional funders, some do attempt direct fund raising from the public and high-net-worth individuals. As noted above, some respondents commented that their GDPR compliance efforts led to a slashing of mailing lists, which in turn limited their capacity to reach financial supporters, while other respondents were circumspect in their reflections, observing that "a smaller mailing list reduced targets although those who did not re-consent were unlikely to donate money." Another issue raised was how to approach potential donors in the absence of an existing relationship. Some NGOs approach high-net-worth individuals to support their work, even using "wealth profiling" companies to identify "targets," and the GDPR has undermined their ability to do this, including by throwing into doubt the legitimacy of the profile service providers.

GRANT MAKING

The answers we received from the survey do not indicate that the GDPR has had a detrimental impact on grant-making practices. In part, this can be explained by the fact that grant making is done through contracts, which can make it easier to address data protection issues and provide a straightforward legal basis as required under the GDPR. Specifically, the GDPR allows you to process data in respect to both the provision and negotiation of services related to a contract. The question of what to do with the data contained in unsuccessful grant applications is more challenging, and organizations retaining data beyond the application process will need to determine that it is in their "legitimate interest" to do so. One action that organizations can take is to implement a wider data protection framework that encompasses, inter alia, transparency toward the applicant and retention periods (see Annex 1). This can be particularly challenging for grant-making foundations that maintain large databases to record grantee and applicant details and to provide their boards with an overview of grant-making activities. These grant databases, especially in the case of larger foundations, also have significant historical value as they constitute an important, detailed record of civil society at any given time. One organization we spoke to is considering cleansing their database of personal data and, over the longer-term, placing the information in a public archive as a record of civil society work. A staff person from another organization explained that "we use a decision tree to determine specific legal clauses for each grant contract."

3. When Non-profits Get It Wrong: Two Examples

Case one

A small NGO conducting research on the role of social media platforms in the spread of disinformation experienced a data breach a few months after the GDPR came into effect. The breach concerned the publication of individuals' Twitter handles clustered according to political leanings—sensitive personal data in this context. At the time of the data breach, the NGO had one full-time employee and three part-time volunteers and GDPR compliance efforts were underway. This major crisis compelled the group to hire a lawyer and speed up its compliance efforts, but the fallout from the breach has been substantial:

- The NGO had to spend a third of its organizational budget for 2018 dealing with the breach, which prevented them from hiring a new staff member. The executive director said, "...we've been forced to work on this as the first priority, preventing us from fund raising or delivering other projects. Without a solid financial background, our organization could not have survived this."
- Staff and volunteers experienced serious online harassment in response to the breach, receiving 250,000 abusive tweets a week at the height of the crisis as well as personal details of staff (home address and private photos) being published online.
- The NGO received around 200 Subject Access Requests following the breach. By reallocating substantial resources, they were able to respond to the requests. Also, given the context of the breach and harassment experienced by staff, it is highly likely that at least some of the requests were made vexatiously.
- The relevant data protection authority made contact immediately after the data breach, and launched a formal (ongoing) investigation a few months later. The NGO is now working with their lawyer on responses to questions from the authority and is expecting to be sanctioned.

LESSONS LEARNED

This case illustrates how NGO vulnerability and the seemingly arcane topic of GDPR compliance are intertwined. Vulnerability is heightened if the NGO is handling large volumes of personal data, but also if the NGO is conducting politically sensitive work. In an increasingly polarized world in which human rights and social justice advocates are targeted by right-wing activists, "hacking," "doxxing" and hostile subject access requests are issues that civil society organizations are likely to contend with on an increasing basis. The case

also provides two more important reminders. First, "open source" does not mean "open season"—as soon an organization incorporates personal data from the internet or other public records into its own databases, it becomes a data controller and the obligations under the GDPR apply. Second, data protection authorities are, in practice, unlikely to show mercy to organizations on the basis of the nature of their work—even to well-intentioned start-up NGOs with barely any staff. Finally, whereas the NGO in this case was able to repurpose existing, unrestricted funds to ensure both GDPR compliance and organizational survival, the case suggests that funders need to take their grantees' information security and data handling practices seriously, in the same way they do financial health and organizational governance. This in turn will require support to enhance organizational resilience.

Case Two

From 2015 to 2017, the United Kingdom's Information Commissioner's Office (ICO) undertook a large-scale investigation into the data management practices of charities, with a focus on their fund raising activities. Serious breaches of the Data Protection Act 1998 were uncovered and 13 charities were issued significant fines. Many of these charities had gathered the personal data of potential donors from third parties offering data-matching services and some pooled data together to trade between different organizations. This data was used to either contact individuals who had donated in the past, but for whom updated contact details were not available, or to "fill the gaps" of personal data available about potential donors. Some charities also engaged third party companies to "wealth screen" potential donors i.e., rank people based on income and assets and their likelihood of making a donation. This resulted in the invasive processing of sensitive data, all without the data subjects' knowledge or consent.[9]

While the ICO issued fines to offending charities that were below the maximum penalty amounts available, all organizations engaged in raising funds from the public were effectively put on notice. Eight charities voluntarily undertook a risk review process with the ICO that involved a detailed audit of their policies, procedures, governance, and data management practices. This gave the charities the opportunity to understand their own compliance status and to proactively prepare for the GDPR, as well as provide the industry with a snapshot of its compliance position as a whole. The strengths and weaknesses of the organizations' practices were detailed in a publicly released report.[10]

9 "ICO Fines Eleven More Charities," *ICO*, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/04/ico-fines-eleven-more-charities/, April 5, 2017.

10 "Findings from ICO Information Risk Reviews at Eight Charities," *ICO*, https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2259675/charities-audit-201808.pdf, April 2018.

LESSONS LEARNED

The audit process revealed themes across the charities in areas of good practice and issues to be remediated. The organizations were typically engaged in data processing activities related to human resources and administration, service users, volunteers, supporters, and donors. Some sensitive data was processed in relation to service users' health, children, and vulnerable people. Most of the organizations had good governance structures in place, appointed data protection officers or established data protection working groups, mapped organizational data flows, and undertaken the process of reviewing and updating staff training procedures. The key areas where rectification was required included:

- **Consent and fair processing:** Most organizations lacked a formal process to give notice to data subjects about how their data would be processed, so consent had not been validly obtained.
- **Third party processors:** Many charities outsourced data processing tasks to third parties, but in many cases contracts containing appropriate data protection clauses had not been entered into. In other cases there was no contract documenting the relationship at all.
- **Policies:** Many charities lacked adequate information governance and incident reporting policies or had failed to make these available for staff and volunteers to review. The audits also revealed that many charities had a lack of policy management frameworks.
- **Training:** Policies were not always communicated effectively across the organizations. This tied into a lack of adequate training for new recruits and "refresher" training for existing staff and volunteers—despite the fact that these individuals are often involved in public interface and frontline data collection.
- **Monitoring and reporting:** Most of the organizations had no routine compliance checks for data protection or direct marketing in place and internal audits were not conducted consistently.
- **Retention and disposal:** There was a trend of holding onto data far longer than necessary, mainly due to poor data management and the need for someone to be appointed to manage and record this process. There were also instances of groups retaining the personal data of previous supporters for long periods in the hopes that these individuals might engage with the organization again.

4. Subject Access Requests: A Disruptive Tool

Under the GDPR, data subjects can seek information about the data held on them by lodging a "subject access request" with a data control-

ler.[11] Subject to limitation where justified, the subject access request confers on data subjects the right to obtain a copy of the data collected about them, understand how it is collected, know why it is being processed and which third parties receive it, review what safeguards are in place to protect transfers, receive an explanation of the logic behind any profiling, and have personal data deleted. With increased control over their data, individuals can be better informed and in some instances may be able to choose to share their data with more discretion. In turn, this encourages data controllers to be more accountable and transparent about how they treat personal data. This is particularly significant for organizations whose businesses are built on data harvesting models.

In the CSO space, subject access requests can impact organizations in several ways. First, these requests can be used as a tool to expose and understand how organizations process personal data. A number of privacy and data protection CSOs engaged in advocacy work have mobilized subject access requests in this way against organizations that are processing data unfairly. As noted earlier, the Cambridge Analytica case cascaded from a single subject access request made by one individual.[12] Second, while the GDPR requires member states to reconcile data protection principles with the right to freedom of expression and information, powerful individuals have already deployed the lodging of requests to interfere in the work of investigative journalists and researchers who are reporting on them, particularly in order to expose or gain access to sources of leaked data.[13] Finally, given the time and resources involved in responding to a subject access request, adversaries or malicious actors may lodge requests against CSOs in an attempt to distract and disrupt their programmatic work. One data-rights focused NGO we spoke to said that they had received numerous subject access requests that they believe were an attempt to derail their work.

Subject access requests used in campaign for workers' rights

Uber drivers in the United Kingdom have lodged subject access requests with the platform in order to gain access to data about their hours spent logged in to the application, the dispatch of rides (including the logic behind the algorithms used to assign these), and other information. Drivers need this data to demonstrate their status as employees rather than freelancers, the actual hours spent working, entitlement to minimum wage, and other employee benefits. This will be a test case in establishing workers' rights in the United Kingdom's growing "gig economy." So far Uber has responded by providing limited datasets to drivers who applied directly to the organization. It has denied a number of requests lodged by lawyers representing drivers on grounds including intellectual property (the alleged need to protect the algorithms that contribute to the function of the platform) and that the data sought may contain personal data belonging to other individuals (i.e., details of passengers' rides).[14]

Subject access requests used to challenge algorithmic decision-making bias

The Open Knowledge Foundation in Germany launched a campaign in 2018 encouraging individuals to make subject access requests to Schufa, Germany's major credit rating agency. Businesses and organizations rely on Schufa to determine an individual's creditworthiness for receiving financial resources such as loans, credit cards, and mortgages. Many individuals have been subject to negative decisions made by lenders apparently based largely on the "personal scores" provided by Schufa. Individuals often do not receive a clear explanation about how the Schufa scoring system works or what information it uses. The Open Knowledge Foundation has encouraged individuals to exercise their subject access request rights and share the responses received. This has allowed the foundation to review the accuracy and fairness of the scoring system and to attempt to find out what kind of data it uses. Based on its review, the foundation asserts that Schufa's scoring system is prone to error and may have relied upon inaccurate data in some cases. The foundation is seeking further explanation as to the algorithm behind the scores. Schufa is at present refusing to provide individuals with free information by email, instead offering only hard copy responses by mail and limited information beyond the individual's personal score. The German Federal Ministry for Justice and Consumer Protection has announced that credit rating agencies should reveal their algorithms, clearly explain these to consumers, and cooperate with civil society groups, journalists, and researchers investigating the issue. The foundation's campaign is ongoing but has been successful in drawing public attention to the need for more transparency around the issue of credit scoring.[15]

11 GDPR Article 15 extending the access rights afforded to individuals under the GDPR's predecessor, the EU Data Protection Directive 1995 at Article 12 and giving effect to the right to data protection as enshrined in the EU Charter of Fundamental Rights at Article 8.

12 "One Man's Obsessive Fight to Reclaim His Cambridge Analytica Data," *Wired*, Issie Lapowsky, https://www.wired.com/story/one-mans-obsessive-fight-to-reclaim-his-cambridge-analytica-data/, January 25, 2019.

13 "Information Commissioner Throws Out Beny Steinmetz Complaint Against Global Witness," *Global Witness*, https://www.globalwitness.org/en/archive/information-commissioner-throws-out-beny-steinmetz-complaint-against-global-witness/, December 21, 2014.

14 "Uber Drivers Demand Their Data," *GDPR Today*, https://www.gdprtoday.org/uber-drivers-demand-their-data/; https://www.economist.com/britain/2019/03/20/uber-drivers-demand-their-data, March 25, 2019; "Uber Drivers Demand Their Data," *Economist*, https://www.economist.com/britain/2019/03/20/uber-drivers-demand-their-data, March 20, 2019.

15 *OpenSchufa: Die Ergebnisse (Updates)*, Arne Semstrott and Walter Palmetshofer, Open Knowledge Foundation Deutschland, https://okfn.de/blog/2018/11/openschufa-ergebnisse/, November 28, 2018; *Handlungsempfehlungen*, Open Knowledge Foundation Deutschland, https://okfn.de/files/blog/2018/10/SVRV_HR-Verbrauchergerechtes_Scoring.pdf, undated.

In Finland, a data subject lodged a complaint with the Data Protection Ombudsman about the personal data relied upon in assessing their creditworthiness by Svea Ekonomi—a financial lending company. Svea Ekonomi provides an online credit decision-making service that the ombudsman found to be an automated decision-making process for the purposes of Article 22 of the GDPR. According to the ombudsman's findings and in line with GDPR, information about the decision-making process and an avenue for human intervention and review must be provided to the data subject. It was also revealed that the scoring system used an upper age limit in determining creditworthiness, i.e., applicants of a certain age and older were immediately disqualified from obtaining credit. In its decision, the ombudsman ordered that the company change its automated decision-making process, declaring that the use of a categorical age limit contravened credit-lending laws and could not alone be used to determine an applicant's solvency.[16]

Establishing the journalistic exemption in respect to subject access requests

Global Witness, a U.K.-based organization engaged in international anticorruption investigation and reporting, has extensively covered the corruption and bribery scandal around BSG Resources Limited's mining holdings in Guinea.[17] In 2014, the company's founder, Beny Steinmetz, and three others associated with BSG Resources made subject access requests to Global Witness under Section 7 of the then Data Protection Act 1998 UK (DPA 98).

Global Witness did not respond to these requests and the data subjects consequently lodged complaints with the ICO and initiated High Court proceedings for breach of privacy and non-compliance with the DPA 98.[18]

Global Witness relied on the public interest journalism exemption within the DPA 98 (an exemption grounded in the GDPR's predecessor—the EU Data Protection Directive 1995) but BSG Resources argued that because Global Witness also undertook advocacy and campaigning work it was not strictly undertaking the processing for the purposes of journalism (i.e., there was a secondary purpose at play tied to Global Witness' social and environmental justice initiatives) and so could not rely on the journalistic exemption. This argument, if successful, would have very serious consequences for the work of Global Witness and other similar organizations.[19]

The issue was deferred from the High Court to the ICO for determination.[20] The ICO confirmed that Global Witness could benefit from the journalistic exemption, clarifying the scope of the exemption by making clear it applied not just to conventional media organizations but also to civil society organizations engaged in journalism and public interest reporting.[21] Significantly, under the GDPR EU member states are expressly required by Article 85 to reconcile data subjects' rights and data protection principles more broadly "with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression." The "journalism exemption" under the GDPR and the relationship between data protection and free speech is discussed further below.

5. Data Protection and Civic Space

Over the past decade, philanthropic foundations and other supporters of civil society organizations have become increasingly preoccupied with the way in which governments, laws, policies, and right-wing think tanks have been pushing back against progressive causes and social justice campaigns around the world.

Examples of the way civic space is impacted include "philanthropic protectionism," which encompasses a raft of government-imposed constraints on the ability of domestic civil society organizations to receive international funding; domestic laws regulating the activities of non-profits more broadly (for example when governments impose onerous registration, licensing, reporting, and accounting obligations on NGOs); and policies and practices imposing restrictions on the rights to freedom of assembly and association (for example by prohibiting demonstrations, using national security laws to restrict mobilization, or militarizing police forces in the name of "public order").[22]

16 "The Data Protection Ombudsman Ordered Svea Ekonomi to Correct Its Practices in the Processing of Personal "Data," *European Data Protection Board*, https://edpb.europa.eu/news/national-news/2019/data-protection-ombudsman-ordered-svea-ekonomi-correct-its-practices_en, April 24, 2019.

17 "Guinea's 'Deal of the Century,'" *Global Witness*, https://www.globalwitness.org/en/reports/guineas-deal-century/, May 13, 2014.

18 "High Court to Consider Data Protection Act Bid to Halt Reporting of Corruption Allegations," Jason Coppel *QC*, Panopticon, https://panopticonblog.com/tag/steinmetz-and-others-v-global-witness-limited/, February 10, 2014.

19 It is worth noting that the journalistic exemption contained in the DPA 1998 was narrow—applying where personal data was processed only for special purposes, including journalism (see s 32(1)). The exemption offered in the current DPA 2018 widens the application of the exemption to instances where the processing is for special purposes, regardless of secondary purposes (see Schedule 2, Part 5, s 26(2)).

20 Through an application by Global Witness under a provision of the DPA 98 that allows a party subject to special purposes proceedings of substantial public importance to request assistance from the office. This provision has been replicated in the DPA 2018 at s 175.

21 "Information Commissioner Throws Out Beny Steinmetz Complaint Against Global Witness," *Global Witness*, https://www.globalwitness.org/en/archive/information-commissioner-throws-out-beny-steinmetz-complaint-against-global-witness/, December 21, 2014.

22 "UK Data Office Says NGO Has Journalist Exemption, Rejects Steinmetz Claim," *Reuters*, https://www.reuters.com/article/dataprotection-steinmetz-idUSL6N0U61HE20141222, December 22, 2014.

Europe is clearly far from immune from these trends—a wide array of new laws, administrative powers, and other tactics are being deployed by a growing number of EU member states in order to apply pressure to and interfere with the work of civil society organizations. We were aware of cases in which data protection laws were being used to try and force investigative journalists who had exposed political corruption to reveal their sources. Because of cases like these, we wanted to explore whether and how data protection laws might be adding to this new generation of restrictions on activism. As a human rights organization, we were also interested in the way in which data protection laws can be used by civil society to push back against encroachments on civic space.

The assumption is that by providing civil society organizations with legal tools that may be used to enhance corporate accountability and check surveillance capitalism, EU data protection law is very much a win in terms of the "enabling environment" for civil society activism. However, in our conversations with those who participated in our research, it also became clear that there are tensions between data protection and other key legal instruments that civil society relies upon in its work and aspirations.

In this section, we provide some examples of the ways in which data protection laws have been abused, how civil society is pushing back, and places where tensions arise. Ultimately, like many laws, the GDPR is vulnerable to abuse and—like other human rights provisions subject to "balancing" tests—open to restrictive interpretation. GDPR expertise, vigilance, solidarity, and advocacy are needed to address these threats.

Romania: GPDR enforcement threatens media freedom

In Romania, the national data protection authority attempted to enforce the GDPR against journalists from the RISE Project[23] who had reported on alleged high-level political corruption. The RISE Project published material leaked in late 2018 that showed a connection between Liviu Dragnea, leader of the ruling Social Democratic Party, and the Romanian company Tel Drum SA.[24] Tel Drum SA is accused of fraudulently obtaining European funds and it is alleged that Dragnea directly benefitted from and assisted in procuring those funds. RISE supported these claims by publishing, among other data, photos and videos of Dragnea and the Tel Drum SA executives on holiday and socializing together.

Shortly after this material was released, the Romanian data protection authority sent RISE a letter[25] demanding details of sources, access to data, and an explanation as to why the subjects of the story were not informed about the leaked personal data prior to publication.[26] RISE was threatened with a fine of up to 20 million euros in case of non-compliance with the request, but responded by declining to reveal its sources as this would be a violation of an integral part of their work as journalists and of freedom of expression. RISE defended not informing the subjects prior to publishing because the material was presented for journalistic purposes and was reporting on a public authority figure. RISE maintained its decision was in line with the exceptions to certain requirements of the GDPR as provided by Romanian law.[27] As of the date of publication of this report, the Romanian data protection authority has not yet responded to RISE.

Other civil society groups stepped in publicly to call out what in their view is a clear misapplication of the GDPR. Privacy International, European Digital Rights, the Romanian Association for Technology and Internet, and 15 other digital rights organizations sent a letter[28] to the European Data Protection Board, the European Commission, and the Romanian data protection authority expressing concern that the GDPR was being used to threaten media freedom in Romania. Supported by Article 85 and Recitals 4 and 153 of the GDPR, the groups argued that the protection of personal data must be balanced against the freedom of information and expression and that investigative journalism is an essential function of a free, open, and democratic society and must be duly protected. The application of the GDPR must also be consistent with the European human rights framework including the EU Charter of Fundamental Rights and the European Convention on Human Rights.[29] The Romanian Association for Technology and Internet also sent a letter to the data protection authority together with other Romanian civil society organizations addressing these same issues and suggesting that there was a political motive behind the action against RISE.[30]

23 *Investigations Rise Project*, RISE Project, https://www.riseproject.ro/, May 24, 2019.

24 See https://www.facebook.com/notes/rise-project/teleormanleaks/1937024593056150.

25 English Translation of the Letter from the Romananian Data Protection Authority to RISE Project, OCCRP, https://www.occrp.org/en/16-other/other-articles/8876-english-translation-of-the-letter-from-the-romanian-data-protection-authority-to-rise-project, November 9, 2018.

26 Purportedly relying on Articles 57, 58 and 14 GDPR; OCCRP Strongly Objects to Romania's Misuse of GDPR to Muzzle Media, OCCRP, https://www.occrp.org/en/40-press-releases/presss-releases/8875-occrp-strongly-objects-to-romania-s-misuse-of-gdpr-to-muzzle-media, November 9, 2018.

27 Article 7 of Romanian Law 190/2018 excludes certain data processing from compliance with the transparency requirements of GDPR Articles 13 and 14.

28 See https://privacyinternational.org/sites/default/files/2018-11/letter%20to%20EDPB%20re%20Romanian%20case%20final.pdf

29 *Data Protection Law Is Not a Tool to Undermine Freedom of the Media*, Privacy International, https://privacyinternational.org/advocacy-briefing/2455/data-protection-law-not-tool-undermine-freedom-media, November 21, 2018.

30 *Freedom of Expression Must Be Properly Understood in the Context of the Protection of Personal Data*, Bogdan Manolea, ApTI, https://www.apti.ro/libertate-de-exprimare-trebuie-inteles-corect-context-date-personale, November 13, 2018.

In January 2019, the European Data Protection Board replied to Privacy International, commenting strongly on the Romanian data protection authorities' actions, advising that:

- the exercise of a protection authority's powers in the protection of personal data must be balanced against other equally important fundamental rights including freedom of the press;
- under Article 85 of the GPDR, it is the responsibility of member states to reconcile the rights to freedom of expression and information with data protection in national implementing legislation and this must also align with the decisions of the EU Court of Justice and the EU Court of Human Rights;
- the data protection authority's powers must be exercised in a proportionate manner, including in the application of fines; and
- judicial remedies are available at a European level against decisions of data protection authorities per Article 78.[31]

Hungary's foreign funding law

In June 2017, the Hungarian Parliament adopted the Law on Transparency of Organizations Supported from Abroad, also known as the Foreign Funding Law, which requires civil society organizations to register as "Foreign Funded Organizations" where they are engaged in humanitarian and social change work and are receiving the equivalent of 22,000 euros or more from sources outside Hungary. This requirement applies regardless of the percentage of total funding the foreign funds make up. Those civil society organizations are required to display this classification on all materials they publish. They are also required to report in detail on the sources of their funding including individually naming and providing location details of the donors outside Hungary who individually contribute the equivalent of 1,600 euros, with the list of these donors made public on a Hungarian government website. Civil society organizations that fail to register can be penalized financially or shut down.

In August 2017, the Hungarian Helsinki Committee and the Hungarian Civil Liberties Union together with 12 other NGOs lodged a complaint with the Hungarian Constitutional Court arguing that the Foreign Funding Law's motive is to stigmatize, create public distrust, and interfere with or abolish these civil society organizations and the work they do. Following a lack of action by the Hungarian Constitutional Court, in December 2017 the NGOs submitted an application to the European Court of Human Rights.

31 *EDPB Reminds National Data Protection Authorities to Exercise Their Powers Proportionally and in Respect of Fundamental Rights*, Privacy International, https://privacyinternational.org/blog/2713/ebpb-reminds-national-data-protection-authorities-exercise-their-powers-proportionally, February 13, 2019; See https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_to_civil_society_organisations_on_romanian_dpa_investigation_en.pdf.

In their submission, the NGOs included a data protection argument that the Foreign Funding Law's requirement to disclose and make public the personal data of individual donors (including the name, country, and city of foreign donors) violates the right to privacy enshrined in the European Convention on Human Rights.[32] The NGOs also referenced Article 9 of the GDPR, which prohibits the processing of special category data such as political opinions and religious or philosophical beliefs, since it is inevitable that publishing the personal data of individuals who support NGOs subject to the Foreign Funding Law will publicly reveal some of this special category data (i.e., their political leanings).

Article 9 of the GDPR does include some legitimate derogations where the processing is for reasons of substantial public interest, proportionate to the ends being pursued, respectful of the "essence" of the right to data protection, and subject to suitable safeguards.[33] The Hungarian Helsinki Committee filings argue that the Foreign Funding Law has no proportionate or legitimate aim to support such an interference with personal privacy. Nor does it have a legal basis under the GDPR; in a democratic state, there is no justification to make and publish a list of individuals who support certain organizations.[34]

In July 2017, the European Commission launched an infringement procedure against Hungary in relation to the funding law. A letter of formal notice was issued, beginning the proceedings and inviting Hungary's response. Hungary has responded to the notice advising that the government intends to maintain the Foreign Funding Law.[35]

Estonia: Data Protection is used to harass a human rights NGO

In November 2017, a complaint against the Estonian Human Rights Centre (EHRC) was made with the national Data Protection Authority. It related to UNI-FORM, a tool for reporting incidents of hate crime against LGBT+ persons developed by a Portugese NGO. The EHRC was in a partnership with this Portugese NGO in an EU project.[36]

Initially, the local anti-gay activists – SAPTK, a very successful Estonian branch of the anti-progressive movement, Tradition, Family

32 ECHR Article 8 provides the right to private and family life, home, and correspondence.

33 GDPR Article 9(2)(g).

34 *What Is the Problem with the Hungarian Law on Foreign Funded NGOs?*, Hungarian Helsinki Committee, https://www.helsinki.hu/wp-content/uploads/What-is-the-Problem-with-the-Law-on-Foreign-Funded-NGOs.pdf, October 9, 2017.

35 *The Government's Response to the European Commission: The "Stop Soros" Bill Is Here to Stay*, Hungarian Ministry of Justice, http://www.kormany.hu/en/ministry-of-justice/news/the-government-s-response-to-the-european-commission-the-stop-soros-bill-is-here-to-stay, September 19, 2018.

36 https://uni-form.eu/welcome?country=EE&locale=en

and Property – started spreading false information about the tool. SAPTK argued that the tool would be used to create a database of homophobes and initially spread this false information on their own portal. The website of the far-right EKRE party also published the information. When SAPTK failed to spread the false information about UNI-FORM into the mainstream media, they submitted a complaint to the Estonian Data Protection Authority, which started an investigation on the basis of its supervisory powers under the Personal Data Protection Act in force at the time, which has now been replaced by a new national law enacting the GDPR. The EHRC was approached for an explanation by the Data Protection Authority.

As a result of these proceedings, the mainstream media became interested in the story and started to cover it, which meant the EHRC had to engage in crisis communications to defuse the situation. They had to submit corrections to news outlets and work to contain the story (reasonably successfully). Fortunately, the EHRC had strong in-house data protection expertise and was prepared to expertly respond to the Data Protection Authority's investigation. It nevertheless caused stress among the NGO's employees and supporters for several months, requiring them to reallocated resources to crisis communications and redirect attention from their substantive work and other pressing issues. In the end, the Data Protection Authority closed the investigation in April 2018 because they could not identify any concrete instances of data protection violations.

Going Dutch

In December 2018, the Dutch Government published the Draft Act on the Transparency of Civil Society Organizations, which is similar in character to Hungary's Foreign Funding Law. If passed, this would require civil society organizations to publish the personal data of certain donors, ostensibly to make public the financial influence being exerted on these organizations, which can indicate their motivations and purposes. Specifically, the draft act is intended to expose and prevent civil society organizations from being associated with "undesirable influences and the abuse of democratic freedom."[37] Among other details, the names and cities of residence of donors whose donations total 15,000 euros or more per year are to be published. Failure to comply with this requirement would result in financial penalties against the organization.

While the Explanatory Memorandum accompanying the draft act indicates that European human rights laws were taken into account in the drafting process, the draft act's requirements would still impinge upon donors' rights to privacy and the protection of their personal data. This would put individuals in a position where they have to choose between making donations of this scale or protecting their private information. If made into law, the draft act would make it impossible to give donations of 15,000 euros or more anonymously to Dutch civil society organizations. Clearly, this could have a drastic impact on the level of funding available to organizations working on contentious or divisive social issues, as well as putting donors at risk of harm by exposing their personal data. Given the current political climate in Europe, this must be seen as a genuine threat.

Civil society actors responded quickly to the call for consultation on the draft act. Among others, the European Center for Not-for-Profit Law, the European Foundation Centre, the Donors and Foundations Networks in Europe, and Data Protection Support & Management all provided commentary highlighting how the requirements of the draft act interfere not only with the fundamental rights of donors, but also with the free movement of capital and the right to funding enjoyed by civil society organizations.

37 *Draft Bill on Transparency of Civil Society Organizations: Foundations and Associations Must Publish Donations and Financial Data*, Meijburg & Co Tax Lawyers, https://meijburg.com/news/draft-bill-on-transparency-of-civil-society-organizations-foundations-and-associations-must-publish-donations-and-financial-data, January 11, 2019.

Freedom of information and data protection

The right to freedom of information forms an integral part of the right to freedom of expression. Freedom of information is grounded in the principle that information held by governments and public bodies should be freely available, in the interests of increasing accountability and rendering internal practices and decision-making processes transparent. Such information may only be withheld and kept private in circumstances where there are legitimate reasons to protect it, e.g., in the interests of protecting privacy and security, both of individuals and the state. There is therefore necessarily tension between freedom of information and the right to the protection of personal data. To expose information that has public importance, it will at times be necessary to make public the personal data of particular individuals, for example in documenting alleged corruption or abuses of power in connection to the behavior or actions of public figures or the discharge of public duties. It is necessary to balance the two rights to ensure that personal data is protected appropriately and that information is made publicly available.

In the context of freedom of information, achieving this balance requires the separation of personal data from information that serves a key issue or that people are entitled to have. The boundaries of this endeavor are being interpreted by national courts and where inter-

pretation of the GDPR itself is concerned, the EU courts. These courts are also interpreting the rights that individuals have over data that has been published by others, particularly in the context of the "right to be forgotten" codified by the GDPR. The EU courts have recently established some important precedents on these issues.

In the ground-breaking "Google Spain" ruling in 2014, the Court of Justice of the European Union found in favor of a Spanish national who had brought an action against Google to have search results about him removed from the search engine's index. The search results related to legal proceedings brought against the individual years prior regarding social security debts – their appearance in search results was impacting his reputation, his position was that the proceedings had been resolved and were no longer relevant and should therefore be removed from search results. The individual initially made a complaint to the Spanish Data Protection Authority, which held that operating the internet search engine made Google a data processor subject to data protection laws, including the exercise of data subject rights and the protection of the individual's right to privacy. The matter eventually came before the EU Court of Justice, which confirmed that Google's Spanish subsidiary was a data controller in this context and that the central issue to be determined was the balance between the public's right to access this information against the individual's right to privacy and the protection of personal data. The judgment found that in this particular case the individual's right to privacy trumped the search engine's right to index the results. The court, however, noted that in general this balance will depend on the nature of the information in question and the interest of the public in having access to that information—which will vary depending on the circumstances, particularly where the data subject plays a role in public life. Notably, the judgment did not require the actual sources of information that the results linked to (newspaper articles and media publications) to be removed.[38]

In 2017, the EU Court of Justice found that in some circumstances, the public's right to know certain information will override the individual's right to privacy, even where this has a negative impact on the individual. An Italian citizen who was director of a liquidated company sought to have his personal data removed from the public register of companies in Italy. He requested this on the basis that the indexing of his personal data here had a negative impact on his ability to sell properties and a sufficiently long period of time had passed since the company's liquidation. The court decided that, in this case, the public's right to know this information was sufficient justification for the individual's name to remain on the register. The personal impact this had on him was not a sufficiently overriding reason to bar public access to the data.[39]

In weighing the importance of data protection against the EU Regulation on Public Documents—the EU's equivalent of a freedom of information act—the court has taken an equally robust stand, endorsing the use of data protection as a means to restrict access to documents. Transparency International, a global anticorruption NGO, has spent many years seeking information about the spending of public funds by members of the EU Parliament on travel and general allowances. The European Parliament responded to its request for access to the relevant documents by declining to provide the information sought on a number of grounds centered around data protection arguments. Parliament representatives stated that releasing this information would compromise the privacy and protection of parliament members' personal data. The parliament found that that there was no justification for sharing such personal data with Transparency International, holding that the public interest in wanting to scrutinize public spending and assess the parliament's control mechanisms in this arena was "too abstract" to be considered a sufficient reason to transfer the information.[40] Transparency International disagreed strongly with this response and brought the matter before the EU Court of Justice. In September 2018, the court found that the EU Parliament is indeed entitled to withhold this information.[41]

Freedom of expression

Freedom of expression is a cornerstone of democratic society that protects journalism, research, and artistic expression—ensuring that information flows to the public and that private entities and public institutions and figures are held to account for their actions. The principles of both privacy and transparency are crucial in carrying out reporting, research, and investigation in this context. On one hand, the right to privacy and data protection shields sources, allowing for sensitive information to be shared without fear of retaliation or reprisal, and ensures that secure communication channels are available for the transfer of infor-

38 *Google Spain SL v Agencia Española de Protección de Datos, Columbia Global Freedom of Expression*, https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/, undated.

39 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, Columbia Global Freedom of Expression*, https://globalfreedomofexpression.columbia.edu/cases/camera-di-commercio-industria-artigianato-e-agricoltura-di-lecce-v-salvatore-manni/, undated.

40 "The General Court Confirms the Parliament's Refusal to Grant Access to Documents Relating to MEP's Subsistence Allowances, Travel Expenses and Parliamentary Assistance Allowances," General Court of the European Union, Press Release 138/18, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-09/cp180138en.pdf, September 25, 2018.

41 "ECJ Rules against MEP Expenses Transparency," Transparency International EU, https://transparency.eu/ecj-rules-against-mep-expenses-transparency/, 25 September 2018.

mation. On the other hand, the purpose of this work is to expose and make known otherwise confidential information that should be in the public domain. Investigative journalism and research are ultimately directed toward ensuring greater transparency and accountability, yet at the same time they rely on the right to privacy and data protection principles in order to do this work. In recognition for the need to find balance between the exercise of these rights, the GDPR requires member states to enact legislative measures that reconcile freedom of information and expression with the right to the protection of personal data.[42] Member states must exempt data processing undertaken for journalistic, academic, literary, and artistic purposes from some of the provisions of the GDPR to the extent that these would interfere with carrying out those purposes.[43]

While the exemption is to be interpreted broadly in national implementing legislation,[44] these exemptions do not provide a data protection "free pass"—personal data must be still be stored and managed securely as all member states have other regulatory requirements that will apply to the operations and data management procedures of media outlets and academic researchers (e.g., professional codes of conduct and ethics, industry standards, copyright, and libel must all be taken into account). Because of the wide scope for derogation given by the wording in the GDPR, these exemptions will apply differently depending on how they are made into law in each member state. It is important for civil society organizations engaged in this work to consult their relevant national implementing legislation to determine the precise scope and application of the exemptions. At this stage, only 18 out of 28 member states have fulfilled their obligation to inform the European Commission as to their implementation of Article 85.[45] The Council of Europe published Guidelines on Safeguarding Privacy in the Media in late 2018. The guidelines address the balance between the right to privacy and freedom of expression and serves as a useful manual for operating within the EU human rights framework.

A recent decision by the EU Court of Justice has consolidated the scope of application of the journalistic exemption, finding that a layperson engaged in blogging (on YouTube in this case, but likely also on other platforms like Twitter and Facebook, etc.) can rely on the protections designed for the media.[46] In the YouTube case, an individual filmed his interaction with police officers at a local police station and later published the video to YouTube in order to make public the alleged illegal conduct of the officers. While the decision was made in relation to the EU Data Protection Directive 1995, the exemption provisions of the GDPR are very similar and in fact broader, to the extent that journalism must only be a purpose of the processing,[47] not the sole purpose of the processing.[48] The decision shows a willingness of the court to interpret the journalistic exemption broadly and can be considered a win for freedom of expression. The broader implications are that individuals who publish personal data for the purpose of journalism may be able to benefit from the exemption without necessarily being tied to a professional outlet, but again this will depend on how member states choose to interpret Article 85.[49]

Whistle-blower Directive (and data)

In the wake of the LuxLeaks, Panama and Paradise Papers, Cambridge Analytica, and Dieselgate scandals, the European Commission put forward a legislative proposal in April 2018 to extend the protections afforded to individuals reporting breaches of EU law. Prior to this, the protections for whistle-blowers across member states were fractious, covering only specific sectors or offenses, with many states lacking any comprehensive protection framework at all.

In early 2019, the EU Parliament and Council reached provisional agreement on the content of the proposed Whistle-blower Directive—a significant step forward in protecting whistle-blowers and a great achievement by civil society advocates. The directive is designed to encourage individuals across public and private organizations to report breaches of money laundering, corporate taxation, data protection, privacy, food, product, environment, and nuclear safety laws. The directive does this by creating higher and new standards of protection for whistle-blowers against retaliation from employers and other actors. The provisions include (i) creating new reporting pathways—establishing a system of safe channels for reporting within an organization and to public authorities; (ii) establishing safer reporting channels—whistle-blowers may disclose to authorities directly where reporting internally could jeopardize later investigation or put the individual at risk of retaliation, or to the media where the organization or public authority fails to take timely action and (iii) preventing retaliation—providing protection in judicial proceedings and against dismissal or demotion

42 GDPR Article 85, which reinforces the exemption that existed in the GDPR's predecessor, the Data Protection Directive 1995 at Article 9.

43 Article 85 GDPR.

44 Recital 153 GDPR.

45 See https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en.

46 Judgment of February 14, 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122.

47 GDPR Article 85(1).

48 Data Protection Directive 1995 Article 9.

49 In France, for example, data protection laws stipulate that only professional journalists (defined by French case law as someone working for a media company) may rely on the exemption. It is therefore imperative that civil society organizations seeking to rely on this exemption are familiar with their national legislation implementing the GDPR.

by employers. EU member states must now align their existing laws or enact new ones that implement the directive's requirements. They will also be required to inform citizens of whistleblowing procedures and protections available to them.

There are several issues where civil society organizations will be looking closely at the implementation of the directive. First, it must be ensured that civil society organizations are recognized as legitimate reporting pathways for whistleblowers. Second, it should be established that civil society organizations have a legitimate basis for processing whistle-blower data, in the same way that public institutions and bodies do. Regardless of how the directive is implemented, all organizations processing whistle-blower data must still apply basic data protection principles to the datasets.[50]

6. Conclusions

6.1 Compliance is viewed as a chance to lead by example, but compliance challenges are real

Compliance is viewed by many organizations as being in line with their organizational values, and a chance to become more data literate and lead by example in how to govern data responsibly. However, it is resource intensive and often requires the engagement of external service providers. This can result in resources being diverted away from programmatic work. This is particularly challenging for civil society organizations that are under pressure to minimize overheads relative to the money they spend on achieving their mission.

While we do not have the depth of data to be certain, it appears that at least some civil society organizations have over-complied with elements of the GDPR—for example by deleting significant amounts data or conducting impact assessments unnecessarily. Among those NGOs we talked to that did over-comply, we were not surprised to find the most egregious instances in countries where governments are harassing civil society organizations. Civil society may also have set a higher bar for compliance because of a perceived need to meet the highest standards in terms of "good governance" at least as compared to other societal actors. Data protection service providers leveraging fears about non-compliance to attract business and media hype around some of the GDPR's requirements may have been another reason for over compliance. This scenario was likely compounded by a lack of clear guidance for non-profits from many data protection supervisory authorities. While some civil society organizations have evidently over-complied, others have led by example taking a risk-based and proportionate approach and ignoring what they considered to be conservative advice by commercial consultants. For example, they decided not to seek consent for the use of contact details for communication with public officials. Had they followed the unfounded advice, the organization's ability to communicate with policymakers—a core part of its mission—would have been seriously restricted. Yet others have taken a "wait-and see" approach before investing significant resources in data protection or their IT infrastructure. As more examples of good compliance become available over time, and as data protection authorities and courts provide clarity on key issues, developing and maintaining good data governance practices should become easier.

6.2 Compliance for programmatic activities may be more challenging than compliance for operational ones

Although many organizations have addressed the more visible data protection challenges with regards to the operational part of their work, few of the organizations that we spoke to appear to have mainstreamed data protection compliance into their programmatic data processing activities. This is significant because the biggest data protection challenges for data-intensive social justice and human rights organizations may be the programmatic activities rather than operational ones. The collection of sensitive personal data about issues such as human rights abuses, corruption cases, and right-wing activism could be a liability as well as an asset for civil society organizations with powerful adversaries. NGOs providing research support services to investigative journalists who may not be able to rely on the journalistic or research exemptions in the GDPR may face significant challenges. These NGOs may face difficulties such as establishing a clear legal basis for processing and implementing appropriate safeguards for data subjects, achieving an adequate level of transparency around their data processing operations, and implementing appropriate technical and organizational measures. Organizations working on the assumption that because their work is in the public interest the associated data processing must be legitimate could easily find themselves in breach of the GDPR, depending upon the jurisdiction in which they operate. While it is clear that the letter and spirit of the GDPR seek to preserve freedom of expression and facilitate research in the public interest, much is left to EU member states in terms of implementation. It is therefore imperative that civil society organizations are confident about their status and position under both national and EU law.

50 The European data protection supervisor has produced guidance for EU institutions on how they should process whistle-blower data, providing safeguards and advice that all organizations processing such data are encouraged to rely upon.

6.3 Subject access requests have not yet been widely weaponized against NGOs

One of the main questions we investigated is whether the GDPR leaves NGOs exposed to action by vexatious and litigious adversaries and has implications for what is now widely recognized as the "shrinking space" for civil society. This question is particularly relevant as risks for NGOs are growing in an increasingly polarized world in which human rights and social justice advocates are targeted by both repressive governments as well as right-wing activists.

In our research, we did come across attempts by hostile governments and groups to use data protection law against NGOs, for example to prevent NGOS from publishing or distributing information revealing illegal activities. Though suppression efforts have been unsuccessful to date, they have in some instances created significant legal hurdles for NGOs. In exploring whether subject access requests are being "weaponized" against NGOs, we have not found this to be a serious threat yet. We only came across one instance where an NGO received numerous requests (following a data breach) that they believe were an attempt to disrupt their work. However, we remain concerned that NGOs may be vulnerable to weaponization attempts, especially where they have failed to establish a clear legal basis and specific purpose for processing the data they hold, or to implement the requisite safeguards.

6.4 Data protection authorities currently do not provide satisfactory guidance for or support to civil society organizations

Our survey suggested that many civil society organizations are dissatisfied with the guidance that has been provided by their national data protection authorities and have faced significant difficulties in obtaining free and relevant advice. While generalized compliance resources are available, civil society organizations have many unanswered questions about how the GPDR applies specifically to their work. The European Union has prioritized outreach and support to small and medium-sized enterprises but has apparently not yet considered the challenges faced by non-profit organizations. In the absence of clear guidance and support, civil society organizations that want to ensure they are compliant are disproportionately burdened—at least as compared to the business community—and left with little option but to expend scarce resources on expert advice. The situation is unlikely to change unless political demands are placed on national and EU data protection authorities and resources are made available to support data protection compliance in the non-profit sector.

6.5 The interpretation of national and EU data protection law will have a significant impact on an "enabling environment" for civil society

While data protection laws may be used to try and limit free speech and expression, particularly in the context of investigative journalism and anti-corruption and human rights activism, data protection is also a core part of the enabling environment for civil society. It allows civil society groups to challenge egregious practices in the private sector and push back on egregious practices and data monopolies. Crucially, because of the intersection between data protection and other tools and constructs on which civil society depends—such as freedom of expression, freedom of association, freedom of information, access to financial services, and effective whistle-blower protection—the way that data protection law is interpreted by supervisory authorities and the courts will inevitably extend or constrain civil society space in subtle but vitally important ways. Almost all sectors of the economy sent professional bodies, trade associations, and lobbyists to Brussels in an attempt to ensure that the GDPR did not affect business as usual while civil society simply pushed for a high bar of data protection, including by pushing back against these private interests. As issues that affect the space and means for civil society to operate, advocate for social justice, and hold the powerful to account are legislated and interpreted, it is imperative that civil society considers its own interests as well as those of others it seeks to defend.

6.6 GDPR compliance and organizational resiliency are intimately linked

Because of the link between legality of processing and vulnerability to vexatious litigation, GDPR compliance and organizational resiliency are deeply intertwined. At a more general level, regardless of the areas in which particular civil society organizations work, data breaches or poor data protection practices can also lead to costly enforcement actions by data protection authorities, as noted in our case studies. In an increasingly polarized world in which human rights and social justice advocates face increasingly well-resourced adversaries, the risks of "hacking," "doxing," surveillance, subversion, and disruption are growing. While different organizations face different threats and levels of risk, good data protection practices including technical and organizational measures to prevent unauthorized access to personal information are a critical line of defense against malevolent actors.

6.7 Links between the responsible data, digital security, and data protection communities need to be strengthened

Data protection is but one of several core digital challenges that civil society has faced

in recent years. However, these challenges are being addressed in a rather disjointed manner. The Snowden revelations and the ramping up of surveillance and political policing have catalyzed significant investment in digital security on the part of numerous NGOs and funders. At the same time, as civil society organizations seek to enhance their impact, many have invested in using data more effectively and responsibly to support their investigations, campaigns, and other objectives. Data protection compliance was added to the mix somewhat later as the 2018 GDPR deadline approached.

Strengthening the links between these communities will be critical going forward. The core data protection principles provide a logical basis around which to orient new data programs and innovations (see best practice section at Annex 1). Good digital security and data hygiene can go a long way in ensuring that organizations implement technical and organizational measures to meet their data security obligations, which are an integral part of data protection compliance. By considering data protection as something to be achieved in practice rather than something with which to comply, civil society organizations will be much better placed to address compliance challenges in their programs and operations, and meet the accountability requirements that the GDPR contains. This will require program staff, data specialists, information and communication technology service providers, and compliance officers to work together from the outset of new initiatives, which may in turn require a cultural shift within particular organizations.

7. Recommendations

For Non-Governmental Organizations

- Data intensive civil society organizations should review their data gathering operations to ensure that they comply with the GDPR. The best practice section at Annex 1 below can serve as a starting point. Civil society organization leadership should in turn properly factor GDPR compliance into their risk assessment for the organization.
- Ensuring data protection is mainstreamed into all data processing operations including the programmatic operations will make organizations more resilient in the face of significant risks to their operations from malpractice. This is far from easy to achieve and requires attention by NGO leadership and the securing of resources for this effort. Ultimately, NGOs will not be able to achieve GDPR compliance if is not prioritized and adequately funded.
- NGO leaders should educate themselves and dedicate resources to supporting their staff in implementing and designing GDPR-compliant practices.
- Umbrella organizations in the non-profit sector should mainstream data protection into their thematic and operational work by addressing policy matters and providing their members with practical tools to meet sectoral compliance challenges.

For funders

- In the short term, funders should think of their grantees' organizational resilience and GDPR compliance as intimately linked. In practice, this means that donors need to add data protection compliance to the list of criteria used to determine organizational resilience and make flexible institutional funding available to help their grantees with GDPR compliance. They should also support data-intensive social justice and human rights NGOs to pair up with GDPR compliance experts to work through some of the particularly thorny compliance questions in a set of diverse contexts, and support a living best practice document and forum where NGOs can find answers to their questions.
- Over the mid-term, funders need to create a more holistic support infrastructure for civil society integrating expertise in data protection, responsible data, and digital security. It is, for example, imperative that the experts making up this support infrastructure follow and engage in debates about the ongoing interpretation of data protection provisions that affect civil society and its operational activities. The responsible data community, given its founding principle of a rights-based approach to data, has an important role to play in fostering connections between these communities of experts. Increasingly, this infrastructure will need to concern itself with the role data grantees are exposed to on a day-to-day basis and how it creates harm (e.g., secondary trauma) and creates an additional risk for organizational resilience.

For data protection authorities

- In consultation with NGOs, the European Data Protection Supervisor, and national Data Protection Authorities should support the drafting of a dedicated data protection handbook for civil society organizations.
- Supervisory authorities must be made to refrain from using data protection laws to unduly restrict the activities of civil society organizations. The European Data Protection Supervisor and the EU Agency for Fundamental Rights should provide updated guidance on the relationship between data protection, freedom of association, freedom of expression, and freedom of information with a view to ensuring an enabling environment for civil society in the European Union.

8. Methodology

This report is the product of three substantive research efforts: (i) desk research and the analysis of guidance on the implementation of the GDPR available to non-profits; (ii) a survey canvassing the views of non-profits on their experience of complying with the GDPR; (iii) semi-structured interviews with representatives of non-profits on GDPR-related topics.

At the beginning of the project, we also spoke with various interlocutors and stakeholders, including data protection bodies and umbrella organizations representing non-profits and civil society groups. The goal was to ascertain interest in the project, validate our approach, and seek assistance in the distribution of the survey and the identification of potential respondents. We also used the conversations to develop the questionnaire, frame specific questions, and pilot the survey.

Through the survey and follow-up interviews, we wanted to know about the investments of time and money that organizations have made in complying with the GDPR. We also wanted to learn about the issues that they struggled with, how they felt about available guidance, where they looked to for help with this work, how the GDPR affected specific areas of work (advocacy, grant making, research and investigation). Another area of our inquiries was whether NGOs and civil society groups had been subject to enforcement actions or received subject access requests, and whether they deemed these to be vexatious or malicious. In the survey, we also left room for qualitative responses. The survey is reproduced in full in Appendix 1.

We sent the survey directly to organizations within the networks of our organizations. We also approached foundations and umbrella organizations to help disseminate the survey including Ariadne—the European network of funders supporting social change and human rights—and civil society support organizations such as the European Centre for Non-Profit Law. Lastly, we distributed the survey via social media and in *GDPR Today*.[51]

Our goal was to reach Europe-based NGOs or NGOs that worked internationally but were subject to the GDPR because they were very likely handling the personal data of Europeans.

The survey was open from late January until early March 2019. We received responses from 52 civil society organizations, the majority of which are advocacy organizations working in human rights and social justice (only two identify as research and education organizations). We had hoped to get a larger pool of respondents but are satisfied that this is a representative sample of target organizations with legitimate concerns and experiences.

Our sample is biased in the following ways, which should be taken into account when reading the report: most of our respondents are small NGOs, i.e., around half of the respondents have 1 to 10 employees and only 4 have more than 50 employees. Twelve respondents are grant makers, the majority are grant seekers, and a small number do both. Almost all respondents (47) are headquartered in the European Union, with the highest number based in Belgium, the Netherlands, and the United Kingdom. We also have good representation from groups in Eastern Europe, but groups from Southern Europe and the Nordic countries are largely absent from our sample.

As most of our survey respondents are advocacy organizations, we aimed to correct for this bias in our sample by conducting post-survey interviews with respondents working in other areas and general information gathering interviews with eight other civil society organizations. These were all data-heavy organizations engaged in substantial investigation, research, and documentation into human rights and social justice issues. Through these semi-structured interviews, we were able to follow-up on survey responses and ask people specific questions about issues of interest.

One word on terminology: We are using the terms non-governmental organizations (most commonly referred to as "NGOs"), non-profit organizations, and civil society organizations interchangeably throughout this report.

Annex 1 – Complying with the GDPR: Best Practices for Civil Society Organizations

When we created this report, we envisaged producing a best practice section based on the responses to the survey and the discussions we had with key respondents. In practice, these conversations yielded more questions than answers. We therefore decided to take a practical and sector-specific approach to compliance issues where there still appears to be a lack of clarity for civil society organizations. Our best practice section is still based primarily upon the outcomes of the survey, addressing the key issues identified by multiple respondents, those that arose during the course of the post-survey interviews we conducted, and some of the gaps identified in the existing guidance.

Rather than restating existing regulatory authority or general advice, the purpose of this section is to share knowledge and build upon the information gathered and lessons learned by the organizations we contacted.While the guidance will be practical and actionable and provide some clarification about how to solve these recurrent issues, it is not legal advice and not intended to be relied upon in this way. Organizations should always first consult their relevant national implementing legislation and regulatory authority advice where available, as well as keep in mind that this is a developing body of law with evolving jurisprudence and regularly updated guidance.

KEY STEPS FOR CIVIL SOCIETY ORGANIZATIONS TO TAKE

- **AUTHORIZE** someone to implement and monitor data protection compliance and ensure they have the support and buy-in from the rest of the organization.

51 "GDPR's impact on the non-profit sector: seeking your input," *GDPR Today*, https://www.gdprtoday.org/gdprs-impact-on-the-non-profit-sector-seeking-your-input/, January 28, 2019.

- **KNOW** what data you hold, what you are doing with it and why—this can be achieved by creating and regularly updating a data processing inventory.
- **ASSESS** the risk level (for both the organization and data subject) of each processing activity and the overall data operations of the organization.
- **PRIORITIZE** compliance efforts based on the level of risk.
- **IMPLEMENT** the core data protection principles using the following steps:
  - have a legal basis for each processing activity;
  - only collect, hold and process data that is demonstrably necessary—each processing activity must have a purpose and the data you process must be tied to that purpose. The common sense application of this principle is to only process data that you can justify having, and if you can't justify why you have it then you need to delete it;
  - keep the data secure, both technically, with appropriate digital defenses, and organizationally, through operational policies and procedures that support data protection;
  - ensure that any data transfers are secure and supported by an agreement or other transfer mechanism where necessary; and
  - be transparent with the data subjects, update privacy policies and information notices to ensure that the data subject would not be surprised to know how their data is being processed.
- **FAMILIARIZE** yourself with the national data protection law in your country and understand how it applies exactly to your organization—there may be relevant exceptions to certain requirements available depending on the nature of work you undertake.
- **REVIEW** your compliance status on a regular basis—this work is not static and the steps above must be undertaken on a continuous basis, keeping up with changes in the data, the organization processes, the activities compliance requires, the hiring of new staff, and changes in law.

Below we set out guidance on steps 1–5 and provide in depth explanations of the legal basis and the policies your organization needs.

INTRODUCTION: WHAT YOU NEED TO KNOW ABOUT THE GDPR

Scope

The GDPR's application is very broad and any entity (person or organization) that meets any of the following conditions will need to comply:

- the entity is located in the European Union and processes personal data in the European Union;[52]
- the entity is established in the European Union and processes personal data as part of its activities, regardless of where the processing itself takes place;[53]
- the entity is located anywhere in the world and processes the personal data of EU data subjects, either linked to selling goods and services or monitoring the behavior of those individuals; and
- the entity is established anywhere else that EU member state law applies by virtue of public international law.[54]

The GPDR will not apply where the processing is strictly for personal or household reasons (e.g., keeping a personal contact list or managing family matters),[55] the activities are outside the scope or EU law,[56] or certain activities undertaken by the European Union an EU member state or law enforcement body.[57]

Definitions

Personal data is defined very broadly under the GDPR and includes any information relating to a living individual that will either identify them (e.g., name, address, phone number, email address, ID or contact details of any kind) or make them identifiable (e.g., location data, IP address or information that relates to the individual's physical, genetic, mental, economic, cultural or social identity).[58] Some types of information are more sensitive than others and there is consequently a higher risk associated with processing this data. This is recognized in the GDPR through the concept of "special category data," which is personal data that is or may be sensitive and includes race, ethnicity, political opinions, religious or philosophical beliefs and details of sex life or sexual orientation. Restrictions are set out in Article 9 that prohibit the processing of special category data unless certain conditions are met. These include obtaining the data subject's explicit consent and ensuring appropriate safeguards are in place to protect data subjects.

Processing is also defined very broadly under the GDPR to the extent that doing pretty much anything at all with personal data will likely fall within its scope—collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, transmitting, disseminating or making available, aligning, combining, restricting, erasing or destroying personal data are all data processing activities.[59] Essentially, where an organization deals with personal data in any capacity, it will be

52 "GDPR's impact on the non-profit sector: seeking your input," *GDPR Today*, https://www.gdprtoday.org/gdprs-impact-on-the-non-profit-sector-seeking-your-input/, January 28, 2019.

53 "Established" here means that the entity has a presence in the European Union, this may apply where an international organization has an office in France but undertakes some or all of its data processing operations to its U.S. headquarters for example.

54 GDPR Article 3(1), Recitals 22, 23, and 25.

55 GDPR Article 2(2)(c).

56 GDPR Article 2(2)(a).

57 GDPR Article 2(2)(b) and (d).

58 GDPR Article 4(1).

59 GDPR Article 4(2).

engaging in data processing. This applies to both internal data (chiefly human resources) and data gathered on other persons (dealing with supporters, donors, beneficiaries, etc.).

It is also important to understand the roles of the "data controller" and the "data processor." The former is the entity that decides what data to process and why, and which entity will be in charge of managing, directing or overseeing data processing operations.[60] Sometimes, two or more entities will make these decisions about the same personal data together and in these instances will be joint controllers in respect of the particular processing activity.[61] The "data processor" is the entity that conducts data processing operations on the instruction of a data controller and can only process personal data in accordance with those instructions.[62] For example, a charity (data controller) contracts an email service provider (data processor) to send out monthly newsletters to its subscriber database (data processing activity). It is quite possible that a single entity could be both a data controller and a data processor in respect of different data sets or processing operations at the same time.

Finally, there are two issues that seem to cause endless confusion on the part of researchers. The first is the use of personal data that is already in the public domain. Whereas many people correctly assume that by publishing information on social media platforms etc., the individuals concerned have largely abdicated their right to privacy. However, it remains the case that if you are collecting and/or re-using this data you are still bound by the GDPR and must ensure that your use of the data conforms to its requirements (see further "open source data," below). The second issue is that while it is also the case that fully "anonymized" data is exempt from the GDPR because it no longer qualifies as "personal data," it is increasingly difficult to "fully and irreversibly" anonymize personal datasets to meet the re-identification test required by data protection law.[63] Moreover, many datasets that that are considered anonymous by their users may still contain a unique identifier that is connected to their real-world identity. Such data is "pseudonymized" rather than anonymized and still falls within the scope of the GDPR. Even if the data has been pseudonymized using techniques such as coding or hashing, basic data protection obligations still apply if it is possible to re-identify the individual data subjects by reversing the pseudonymization process.[64] These obligations only cease to apply when the data are fully and irreversibly anonymized.

60 GDPR Article 4(7).

61 GDPR Article 26.

62 GDPR Article 28(3)(a).

63 *Anonymization:* Managing Data Protection Risk Code of Practice, ICO, https://ico.org.uk/media/1061/anonymisation-code.pdf, November 2012. Note – this document is currently being updated by the ICO.

IMPLEMENTING THE KEY STEPS

1. Give responsibility to people in your organization

Even though small organizations may be exempt from appointing a data protection officer, it is crucial that key staff within the organization make data protection their responsibility, and that any data protection risks are properly identified, brought to senior management, and that action is planned to mitigate them. Creating a data protection working group is one solution that ensures that knowledge is spread throughout the organization, rather than sitting with one person, and for larger NGOs, that the different needs within the organization are represented.

Appointing a data protection officer is mandatory in any of the following cases:

- you undertake large-scale, regular and systematic monitoring of individuals as a core part of your work;
- you undertake large-scale processing of special categories of data or data relating to criminal convictions or offenses as a core part of your work; and
- you are a public authority or body (except for courts).[65]

While a specific determination of what is "large scale" in this context is not available, certain factors should be taken into account including (i) the number of individuals concerned, (ii) the amount and type of data involved and (iii) the scale of processing activities (what the data is used for and how long it is retained, etc.).[66] In short, where an organization's work requires the processing of a lot of personal data on a regular basis, and especially where some of that data is sensitive, then a data protection officer should be appointed and given the resources and management support to discharge their responsibilities.[67]

Even where appointing a data protection officer is not mandatory, an organization can choose to appoint one voluntarily. For all organizations, whether or not a data protection officer is appointed, data protection needs to be someone's job. For small organizations, regular review of policy and practice by a competent staff member may suffice; in larger organizations it will be more appropriate to share data

64 Through these processes and depending upon how the keys/codes are handled, it is quite conceivable in practice that data may be pseudonymized by one data controller and made available to another in an effectively anonymized format.

65 GDPR Article 37.

66 Article 29 Working Party Guidelines on Data Protection Officers (DPOs) adopted December 13, 2016.

67 *Data Protection Officer (DPO)*, European Data Protection Supervisor, https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en, undated.

protection responsibilities across management and operations. For more complex data protection issues, such as the governance of data sharing between organizations, which may require data sharing or controller-processing agreements, you should consider developing a "toolkit" containing step-by-step guidance and model agreements.

2. Establish a data processing inventory

Creating a data processing inventory (also known as a record of processing activities) allows you to map what, how, and why personal data is processed by your organization.[68] Although it is not mandatory for all organizations,[69] producing the inventory will help you rationalize your data processing operations by providing an overview of the personal data your organization is processing and a basis for assessing its legitimacy. It will also help you improve or implement appropriate data governance and meet some of the key accountability components of the GDPR. Both the French (CNIL) and Belgian data protection authorities have produced helpful inventory templates that show the kinds of information that should be included in the inventory.[70] We have also included a template inventory at Appendix 3 that some organizations have found helpful.

The data processing inventory should detail:

- **Each data processing or set of data processing operations and the categories of personal data involved:** It is not essential to identify each and every processing operation from the outset, but organizations should at least have an overview—even if data processing tasks undertaken for the same purpose are grouped together into single operations. For example, it may be sufficient to group all human resources tasks together as one data processing operation (i.e., payment of salaries, recording availability and leave, health and emergency contact data, performance evaluations and so on).
- **The legal basis for processing:** You need to be confident you have a legal basis to support each processing operation/activity. Guidance on determining and relying on particular legal bases is provided further below.
- **The specific purpose of the processing:** You also need to ensure that you know and have specified the purpose for which you are collecting the data, and that the data collected is necessary to fulfill that purpose. If you do not have a specific purpose for retaining the data then you do not have an appropriate basis for processing it. If you are holding data you don't need then you should consider deleting (or, if justified, archiving) the data and changing data collection practices going forward.
- **Access controls:** You should also detail who has access to the data within the organization and why. Only staff who need access to personal data for the purposes for which it is processed should be able to access the data in practice; sensitive or "special category data" should be subject to strict access controls.
- **Retention periods:** As noted above, you should establish retention periods for all of the personal data that your organization processes. If data is only needed for a limited period, or is no longer actively processed, procedures should be in place for deleting or archiving the data pursuant to the retention schedules. If data is needed on an ongoing basis, it should be subject to periodic review to ensure that it is actually necessary and proportionate to keep it.
- **Processing modalities:** For each data processing operation/activity, you should also document the tools, systems, and software you are using to process the data and ensure that the contracts in place with these providers are GDPR compliant (this includes everything from database software and word processors to physical data destruction services). There are particular requirements in place for the terms and conditions of contracts between controllers and processors set out in Article 28 of the GDPR. If you have concerns, reach out to the third party and ask questions.
- **Data transfers:** You should also maintain a record of personal data that is transferred to partners and service providers. The GDPR contains strict rules for such transfers and you should ensure that data transfers are subject to appropriate governance mechanisms and safeguards (see further below).
- **Data security:** The inventory should also confirm that there are sufficient technical and organizational security measures in place to protect the data (this includes establishing appropriate policies, training staff, and ensuring there are appropriate digital and physical safeguards around data). It follows from the risk-based approach that the greater the risk to the data subject of unauthorized access to the data, the greater the level of data security the controller needs to implement. Given the need for civil society organizations to protect their data from hackers and surveillance, good data security is essential. This requires good information security including access controls and encryption, as well as good "digital hygiene" on the part of all employees.

The inventory should be a living document that is subject to regular review and update.

3. Assess the risk level

The GDPR presents two significant departures in the approach of its predecessor, the EU Data Protection Directive of 1995. First, there has been the move away from a "checklist" based approach, which required organizations to meet key requirements such as registration

68 GDPR Article 30.

69 GDPR Article 30(5) exempts organizations with fewer than 250 employees who are engaged in low risk data processing only.

70 See the CNIL inventory template https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles (in French) and One Trust's unofficial translation to English of the Belgian Data Protection Authority's inventory template available here https://www.onetrust.com/belgian-dpa-publishes-template-article-30-records/.

with a supervisory authority. The GDPR takes a risk-based approach that makes organizations that handle personal data responsible for establishing a level of data protection that is proportionate to the risks posed to data subjects if their data is accessed unlawfully or otherwise misused. The second significant change is a focus on accountability for data processing. This means organizations need to demonstrate their compliance. More than half of the articles within the GDPR imply some kind of accountability component. The GDPR also enhances the level of transparency that organizations processing personal data should attain.

The best way to meet these challenges is to properly identify higher risk processing operations, document the compliance efforts that have been undertaken to ensure respect for data subjects' rights, and provide an appropriate level of transparency toward those affected by the data processing. To borrow a phrase coined by data protection consultants, "Say what you do, do what you say, and be prepared to justify it to a regulator." In the event that your organization is subject to complaints from data subjects or investigations by a data protection supervisory authority, being able to explain how and why data is processed and protected—and to demonstrate this in practice—will provide the best mitigation. It is not enough to theorize about such practices. You need to have effective policies in place and staff whose responsibilities include data management and protection.

4. Prioritize compliance efforts based on risk–level

Different organizations will clearly have different data protection compliance needs that reflect the amount and sensitivity of the personal data that they process. For instance, small non-profits that are only handling data on their staff and supporters, and only minimally processing data about other people should not have much difficulty complying with the GDPR. They need to ensure that they have a legal basis for all of the data they hold. They also need to ensure that the data is collected for a specified purpose and only used for that purpose, and that any "consent" based processing covers the following: respects private subscribers or supporters, meets the minimum standards for "informed consent," has transparency of processing, and allows subjects to withdraw their consent. Further advice on these issues is provided below.

For more data intensive operations concerned for example with the investigation, research, and/or documentation of human rights and social justice-related issues, and in particular the role of individual persons in specific cases, issues or campaigns, compliance is inevitably more challenging and complex. These challenges include determining an appropriate legal basis and specified purpose for the data being used in the "public interest" or "journalistic work." The challenges also include applying data protection principles including "data minimization" to ensure that groups collecting and holding data only process the data they need, and meet transparency requirements where data is not collected directly from the data subject. These determinations should guide operational policy and practice in order to ensure compliance with the GDPR. Staff members and associates who collect and use the data should be centrally involved in the elaboration of these policies, together with those responsible for managing and securing the IT infrastructure. While there is much overlap between information security and data protection, it is now essential to factor the latter into the former through "data protection by design and default" processes that consider the use as well as the security of new systems. While it is far from easy, these kinds of compliance efforts, when done properly, can improve the efficiency and effectiveness of organizations by rationalizing data collection and enhancing data governance.

5. Understand and implement the core data protection principles

The GDPR sets out seven data protection principles. These are common sense standards that should guide all responsible data collection:

- **Lawfulness, fairness, and transparency:** For data processing to be lawful, it must be based on one of the "legal bases" set out in the GDPR (see further below). Processing must also be fair to the data subject. The processing may still have an adverse impact on the individual concerned, but that impact must be justifiable; data processing is unfair if it has an unjustifiably negative impact. Data processing must also be rendered transparent to data subjects, either at the point the data is collected from them, or, where data is not acquired directly, within one month of its acquisition (there are several exemptions to this requirement, see further below). Data subjects may not be misled and should not be surprised by data controllers as regards the nature of the processing.
- **Purpose limitation:** This means that data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes (note that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is considered compatible with the original purpose).
- **Data minimization:** This means that the actual data processed in relation to the specified purpose must be adequate, relevant and limited to what is necessary to achieve the purpose. Necessity has a proportionality component, which means that the purpose should be achieved in the least invasive way available to the controller. The data minimization principle should be applied to every aspect of the processing, i.e., from collection, access, and retention to transferring and archiving.
- **Accuracy:** This means that the data you process must be accurate and, where neces-

sary, kept up to date. if there are doubts about the accuracy of the data being processed, it may still be legitimate to keep it as long as you have a legitimate basis and purpose for doing so. The data, however, should be marked as potentially unreliable.

- **Storage limitation:** This means that you may only keep personal data as long as you need it for a specific purpose. Retention periods should be established, justified, and documented. Data should be periodically reviewed and deleted or anonymized in the event that it is no longer needed. Data may be retained following the expiration of the retention period if it is needed for archiving purposes in the public interest, scientific or historical research, or statistical purposes. If it is to be archived it should undergo a minimization review and wherever appropriate, subject to psuedonymization or anonymization.
- **Integrity and confidentiality (security):** As noted above, you are required to adopt appropriate technical and organizational measures to protect personal data following a risk-based approach. While you may take into account the costs of applying data security measures when deciding what measures to implement, these measures must be appropriate to both your circumstances and the risk the processing poses. Where appropriate, you should look to use measures such as using pseudonyms and encryption. You should also ensure that data is backed up and that procedures are in place to test your back-up procedures.
- **Accountability:** As noted above, you must have appropriate measures and records in place to be able to demonstrate your compliance with the data protection principles and the requirements of the GDPR. Establishing a data processing inventory is a key first step (see further below).

DETERMINING THE LEGAL BASIS

As noted above, a legal basis is required for all data processing that falls within the scope of the GDPR and while there are six legal bases available[71] (see table below), the idea that consent is somehow more important than the other legal bases continues to cloud many organization's thinking on this issue. In practice, alternative legal bases will likely be more appropriate or relevant depending on the context of the data processing and the relationship between the data subject and the data controller.

In determining the legal basis supporting a processing activity, it is advisable to consider all applicable bases and document the reasoning supporting the decision making process. There may be situations where two or more legal bases are applicable and all of them should be recorded as supporting the activity in order to strengthen the rationale for the data processing. The key issues to consider here are why the data are being processed and whether or not the processing falls within the scope of what is envisaged by the GDPR. In most cases, answering these questions should lead to a clear indication of which basis or bases may fit, but at times it may not be clear cut.

Crucially, some of the civil society organizations we engaged with appear to be over-reliant on the premise that the work they are engaged in is broadly in the "public interest." This implies that this somehow provides a legitimate basis for all of their programmatic data processing activities, or even that the organization was somehow "exempt" from complying with the general principles and requirements of the GDPR. This is not the case. The "public interest" basis for processing is defined quite restrictively, and requires data controllers to meet several important criteria (see further in the table on the following page). Organizations will only be exempted from compliance where and to the extent that a relevant exemption applies, not on the basis of the nature of the work it undertakes. As discussed above and explored further below, certain exemptions are available for journalism, academic work, and artistic and literary expression, but this will depend on the national implementing legislation in the relevant member state. It is imperative that civil society organizations are confident that they are processing data in accordance with a legal basis and that any exemptions they rely upon are codified into national law.

71 The other legal bases are consent, performance of a contract, compliance with a legal obligation, protecting the vital interests of the data subject, public interest, and legitimate interest (GDPR Article 6).

Overview of Application of Legal Bases

Legal basis	GDPR definition – Article 6	Application
Consent	(a) the data subject has given consent to the processing of their personal data for one or more specific purposes; See also Articles 7, 8, 9 and Recitals 32, 42, 43, and 171.	Only valid where consent can be freely given by fully informed data subjects before the data is processed. This means that consent will NOT be an available legal basis where an individual can't make a real choice—e.g., when personal data is processed by an organization providing humanitarian aid or other vital services (food, money, accommodation, medicine, etc.) and the data subject has to provide their personal data in order to receive the items. This isn't a real choice for a vulnerable person in need of assistance because their consent cannot be freely given. This legal basis will also be invalid where there is a significant power imbalance between the parties that makes the data subject unable to freely give their consent—e.g., in the context of employment an employee may not always be able to freely provide their consent to their employer because they may be concerned about how the situation could impact their job security. In the above examples, the data processing may still be allowed to occur, where it can be supported by a different legal basis and it can be ensured that there is no disproportionate interference with the data subject's rights and freedoms.
Performance of a contract	(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; See also Article 20.	This basis applies where a contract is being entered into between a data subject and data controller, e.g., for the provision of goods and services.
Compliance with a legal obligation	(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	In certain contexts, personal data must be processed to meet a particular legal obligation (e.g., for employment law and taxation purposes). Data processed for safeguarding purposes, or for "due diligence" procedures to comply with money laundering and terrorist financing regulations would also be covered here, as would compliance with a judicial warrant compelling disclosure of personal data.

Legal basis	GDPR definition – Article 6	Application
Vital interests	(d) processing is necessary in order to protect the vital interests of the data subject;	Vital interests can be relied upon where personal data must be processed in order to protect an individual's life and the person is incapable of giving their consent (e.g., where a person is unconscious and you reach into the pocket to get their driver's license to look for contact or health details). If the processing can be undertaken in a less intrusive way, then this legal basis will not be available. This cannot be relied upon to process health or other special category data if the individual is able to give their consent, but refuses to do so—for example where a person needs medical attention and details of any existing health conditions are required from them, but they decline to share this data then the vital interest basis can't be used to override the individual's decision. When relying on this basis, it is important to document the circumstances so that the decision and reasoning can be justified.
Public interest	(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	Where the organization can demonstrate that the processing is carried out in the performance of a specific task that is in the public interest AND is supported by a mandate set out in law, then this legal basis will apply. Whereas organizations providing humanitarian or other social assistance in accordance with a legal mandate or provision of IHL have been able to rely on the public interest, it is not a justification for data processing by public interest organizations.
Legitimate interest	(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. See also Articles 13 and 21 and Recitals 113, 47, and 48.	This basis may be relevant for data processing undertaken in the course of carrying out work in the organization's legitimate interests, e.g., in the course of undertaking public advocacy and reaching out to decision makers and other stakeholders, or research and documentation work activities. When assessing whether the "legitimate interest" basis is appropriate, a Legitimate Interest Assessment (LIA) should be conducted, allowing you to weigh the benefit to the organization against the impact on the rights and freedoms of the data subjects. The former cannot outweigh the latter, and it must be clear that there will be no undue impact on the data subjects. This legal basis can apply in a variety of contexts, so long as the above preconditions are met and you are confident that the reasoning behind your LIA can support your decision to rely on it if questioned by a data subject or regulatory authority. One of the key requirements when relying on legitimate interest is to never surprise the data subject—that is, if the processing is well outside the bounds of something a data subject would reasonably expect to happen to their data then this is an indication that the legitimate interest basis may not be relied upon in this case.

LEGAL BASES FOR SPECIFIC PROGRAMMATIC OPERATIONS

Research and publication data: Can you rely on the journalism exemption?

Organizations conducting journalistic work and intending to rely upon the exemption provided in Article 85 must:

- Consult national implementing legislation to ensure that an exemption has been provided in the relevant member state law. At the time of drafting, 10 member states have not made notification to the European Commission about how the exemptions have been made into national law, which means it is possible that there is data protection or other legislation in place that applies to journalistic work and has not been updated to reflect the exemptions as made in the GDPR. In the case of any disparity between these laws, the regulatory authority and relevant professional associations should be contacted for advice;
- Make sure that your work falls within the definition of "journalism" as set out in national law and that you meet any additional requirements—e.g., in the United Kingdom, the data processing must be undertaken with the intention to publish the work and with a reasonable belief that the work is in the public interest;
- If working with leaked personal data from a whistle-blower, be aware of how the Whistle-blower Directive may impact this. Where a whistle-blower leaks information directly to a journalistic outlet, the protections of the directive may take effect to protect the action of the whistle-blower, while the publisher may be exempted from the requirements of the GDPR through Article 85—but again national implementing legislation must be consulted;
- Ensure that you have adequate technical and organizational security measures in place to protect the data;
- Comply with any other professional obligations as they may apply;
- While the exemptions that the GDPR has provided are quite broad in principle, it is essential to know how the relevant member state law applies to your organization's data processing so that you can effectively respond should you be faced with subject access, deletion or other requests from data subjects that you may be exempted from having to grant;
- If in doubt, follow the advice on the European Data Protection Supervisor on the application of data protection provisions to whistle-blower data.[72]

RESEARCH AND DOCUMENTATION ACTIVITIES—ENSURING YOU HAVE A LEGAL BASIS

Civil society organizations not relying on the journalistic exemption, or those that are unsure that the exemption can be applied to all of their research and documentation activities, must ensure that they have a legal basis for all of the personal data they process in this context. As noted above, unless your organization is established by a legal charter or specifically tasked with an activity that requires the processing of personal data by statutory legislation, you should not rely on the "public interest" legal basis set out in the GDPR, regardless of the actual public interest in your work. Instead, you should use the "legitimate interests" basis in the context of pursuing your mission or implementing your mandate. In doing so, you must ensure that your interest in processing the data does not override the fundamental rights and freedoms of the individuals concerned. This determination will depend upon what you intend to do with the data and the implications for the data subjects. As noted above, you should begin by (internally) documenting the rationale behind any legitimate interest determination, and ensure that it does not override the rights and freedoms of the data subject. For organizations whose processing activities are expressly designed to identify abuse of power or criminal activity—activities that clearly have the potential to undermine individual rights and freedoms—it is crucial that safeguards are implemented to ensure that data is accurate, relevant, necessary, and proportionate, and that the data is subject to a high level of security.

Researchers conducting in-depth research such as interviews of data subjects may also rely on the consent of the interviewees to the extent that such consent is fully informed and freely given. For consent to be legally valid, the data subject must be furnished with comprehensive information about the intended processing and a record of the consent must be retained by the data controller. The requisite information to be provided to the data subject is as follows:

- the identity of the data controller and, where applicable, the contact details of the data protection officer;
- the legal basis and specific purpose(s) of the processing for which the personal data will be used;
- the data subject's rights as guaranteed by the GDPR and the EU Charter of Fundamental Rights, in particular the right to withdraw consent or access their data, the procedures to follow should they wish to do so, and the right to lodge a complaint with a supervisory authority;
- any automated decision-making activities, including profiling;
- information as to whether data will be shared with or transferred to third parties and for what purposes; and
- how long the data will be retained before they are destroyed.[73]

72 See https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en.

73 If the data subject is already in possession of particular information categories, you need only provide the information that is newly relevant when collecting further data.

The data subjects must also be made aware if data are to be used for any other purposes, and any legitimate interest pursued should be spelt out. Data subjects must also be notified if data is to be transferred to organizations outside the European Union.[74] Importantly, if the data processing entails potential risks to the data subjects' rights and freedoms, the subject must be made aware of these risks during the informed consent procedure.

COLLECTING "OPEN SOURCE" DATA

Even where information comes from a public source ("open source data"), it may still be considered personal data under the GDPR and the obligations to appropriately protect the data will still apply. This is because once you collect personal data that was published by an individual or another entity for a certain purpose and process it for your own purposes, you become a controller of that data. Some of the organizations we spoke to, conduct research that involves collecting the personal data of private individuals from public sources like social media accounts. Although in this context the information has been willingly published by the data subject, that individual would not necessarily have expected or intended that their data would later be collected and processed by a separate entity for another purpose. Regardless, the bottom line is that organizations processing open source personal data are data controllers under the GDPR and the data subjects' rights must still be upheld here.

Practically, this means that you must determine a legal basis for the processing, specify the purpose(s), set appropriate retention periods, and ensure that all the data collected is explicitly related to the purpose(s) and only retained as long as it is needed. Crucially, you must also render the data processing transparent to the data subjects. The GDPR stipulates that where data is not acquired directly from the data subject and is, for example, acquired from a third party or collected from public records or social media platforms—data subjects must be informed about the processing by the controller within one month (or if the purpose is to contact the data subject, when the context takes place). Importantly for civil society organizations collecting and utilizing open source data for their research and documentation, there are two important exemptions to this requirement. The first is the level of difficulty and expense involved in contacting the data subjects—"in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes." While data protection authorities are beginning to enforce these provisions, there are no firmly established rules here. However, it follows that where it is relatively straightforward to contact the data subjects, for example, if you have their email address, this is eminently feasible. Conversely, if the dataset does not include contact details and it would entail significant effort and therefore cost to obtain them, the exemption may be relied upon. The second exemption allows data controllers to elect not to contact the data subject if it would "render impossible or seriously impair the achievement of the objectives of [the] processing." In this instance you must still take appropriate measures to "protect the data subject's rights and freedoms and legitimate interests," including making the information publicly available. For organizations processing open source data at scale, it is strongly advisable to maintain an inventory of the data sources and be transparent about their use. In practice, people whose data may be included should be able to ascertain that this may be the case and seek to enforce their rights as data subjects should they wish to do so. Finally, whenever you are engaged in research and documentation activities, it is advisable to conduct a "data minimization" review. Ask your researchers to review (and document) the extent of the personal data being processed, with a view to ensuring that it is necessary, proportionate, and legitimate in the context of the specified purpose for which it is being collected. This is particularly important where sensitive ("special category") data is processed. Ultimately, if you cannot justify the data collection in the context of your overall mission and specific research objectives, you risk processing data unlawfully.

ADVOCACY

Organizations engaged in advocacy work can reach out to public officials and other relevant stakeholders such as NGOs, associations, and companies without having to first get their consent, where they can demonstrate that this is within the organization's legitimate interests. This type of communication should be considered as distinct from engagement with subscribers, supporters, and other parties, and is legitimate where it forms a critical part of the organization's work and purpose. When contacting people for advocacy purposes it is in principle still necessary to conduct a legitimate interest assessment, but in reaching out to public officials and other stakeholders in the course of social justice advocacy, the data processing is unlikely to be deemed to have disproportionate impact on the data subject. If contacting named individuals directly, it is important to state the purpose and justification for the communication and, in the event that the recipient objects to the contact, to handle the response appropriately in accordance with your obligations to the data subject (see further below).

GRANT MANAGEMENT

As noted above, the performance of a contract provides a solid legal basis for the processing of data related to grant applications, and where a grant agreement is entered into, processing grantee data related to the grant's implementation and review. The issue of what do with this

74 GDPR Articles 12 and 13.

data in the longer term may appear less clear-cut, particularly where grant applications are unsuccessful. This does not, however, mean that you do not have a basis for retaining data related to the application. The following factors should be taken into consideration:

- Do you need to keep data for the purposes of compliance with due diligence obligations, accountancy, financial audit or review? If you are required to keep the data in order to comply with a legal obligation, then the legal basis for retaining the data is clear.
- It may also be in your legitimate interests to retain data about grantees for the purposes of facilitating further applications, or to maintain a historical record or archive of your grant-making activity.
- When keeping grantee data for the purposes other than performance of a contract or compliance with a legal obligation—and indeed for these purposes—it is crucial to (i) conduct a data minimization review to ensure that only the data that is needed to meet whatever objective is fulfilled by the retention; (ii) set a retention period; and (iii) render your practices clear to the data subject at the point of application and contracting.
- In minimizing the data processing, you should also restrict access to the data to those people in the organization who actually need access to the data. If data is held for compliance or archiving rather than operational purposes, access should be further restricted to the extent that it is no longer "actively processed."
- If archiving grantee data, establish clear rules for the transfer of data to the archives, including data minimization, and access controls to the data therein. If you do intend to make the data available to persons outside the organization, procedures should be in place to remove personally identifiable data, or if this is not possible, to seek the permission of the data subject prior to disclosure. Again, having clear, transparent policies about what will happen to grantee data from the outset is crucial. If you are planning to archive the data for historical reference, make applicants aware of this fact and the safeguards you will employ from the outset.

POLICIES—WHAT YOU SHOULD HAVE IN PLACE

- **Privacy policy**—a public-facing privacy policy governing the management of personal data needs to be produced and made available to data subjects to inform them about how their data is being dealt with in order to comply with the transparency requirements of the GDPR.[75] The specific content of this policy will depend on how and why the organization collects and processes data but at minimum it will need to be easily accessible and straightforward. Such a policy will cover:
  - who the organization is
  - what data is being collected from data subjects
  - why and how the data is being processed
  - who the data is being shared with
  - how data subjects can exercise their rights under the GDPR
  - details of how to seek further information, including the data protection officer's contact details where one has been appointed.

  If your organization collects data about people on a basis other than consent, for example in the context of human rights research, investigative journalism or the processing of open source data, then a transparency statement should also be incorporated into the privacy policy to support those activities. In this way, the data subjects who may be affected by this work can understand what is happening to their data and seek recourse or further information if required. The use of "open source" data is discussed further above in this section.
- **Overarching data protection policy**—in addition to public-facing policies, there should also be an internal policy that sets out the procedures in place to apply the data protection principles and accountability requirements into practice across the organization's operations, addressing issues like retention periods and setting out a data breach response plan. This can be achieved either by incorporating data protection principles into existing operations policies (e.g., policies around beneficiaries, human resources, and other key areas of work) or by producing an overarching internal data protection policy for the organization. While this is not required under the GDPR, producing an internal policy will allow you to explain and document how you are implementing or meeting the requirements of the GDPR and provide an operations guide to help staff understand their responsibilities in helping the organization meet its data protection obligations. Applicable safeguards should be explained to data subjects upon request.
- **Cookie policy**—websites using cookies need to have a cookie policy that explains what cookies are dropped by the website, what data is collected, how and why this data is processed, and how data subjects can control those cookies. This may be achieved through a tool or platform that allows individuals to manage these settings. In addition to providing granular control and requiring the user to opt-in rather than opt-out, the best cookie policies explain why the organization uses particular cookies. A good policy will also set out the implications for the user of allowing the cookie onto their device and who will have access to the data compiled by the cookie.
- **Mailing list policy**—post-GDPR, data subjects must actively consent to join your email list. Meeting the minimum transparency requirements outlined above and implementing a two-step procedure that requires an email confirmation on the part of the data subject that they do indeed wish to join the list is the best way of mitigating against potential complaints engendered by mistakes or malpractice. Data subjects must be informed of their right to opt-out

75 GDPR Article 12.

of non-essential communications at any time and be provided with an easily accessible way of doing so. This information should be included in any subscriber correspondence as well as within the organization's privacy policy.

- **Data sharing policy**—sharing personal data between organizations, or passing it to third parties such as researchers, consultants, lawyers or service providers poses numerous data protection challenges. While standardized data sharing clauses can be implemented to govern controller-processor relationships, for example where an organization uses third party solutions to store or analyze data, other relationships can be more difficult to work through. Primarily, you must ensure that you have a specified purpose and legal basis for the data transfer, and ensure that the recipient only uses the data for that specific purpose. You should also document all data transfers, and ensure that data is returned or verifiably deleted by processors when it is no longer needed for the purpose for which it was transferred. If you are dealing with contractors, dedicated data protection provisions can be included in your agreement with them. If you are engaged in a joint research or advocacy project, where different organizations may process the data for different purposes, you may need a formal "joint controller" agreement. Such an agreement will set out your agreed roles and responsibilities for complying with the GDPR. While the joint controller relationship does not require an actual contract to be in place, the arrangement must be transparent to the data subject, and individuals must be able to exercise their rights against each controller. Because joint controllers may be jointly liable for damages caused by the processing, it is crucial to have some form of agreement in place. If your organization routinely shares personal data with contractors or partners, you should consider establishing standard operating and record-keeping procedures to ensure that staff are aware of their data protection obligations and provided with the tools and templates and they need to meet them.
- **Data breach policy**—given both the implications for data subjects and the enhanced enforcement powers of supervisory authorities, it is imperative that staff understand how to identify and respond to a data breach. The former can be achieved through basic training and should be integrated into an information security awareness program that takes into account the most common ways in which data breaches happen as well as the tactics used by "hackers" and other adversaries. The latter requires your organization to be able to detect breaches and have a plan in place should a breach occur. At the very least, this plan should cover how your organization will contain and respond to a data breach. Such a plan should include guidance on when it will be necessary to report the breach to a regulatory authority and the data subjects themselves, and how this will be done. The GDPR requires you to report a data breach to the relevant supervisory authority within 72 hours, depending on the likelihood and severity of the resulting risk to people's rights and freedoms. If there is a high risk of adverse impacts, you must also inform the data subjects themselves "without undue delay." Regardless of whether you are required to notify the supervisory authority or not, you must keep a record of all data breaches. Requiring staff to report even the most minor of data breaches to a data protection officer or focal point is a good way of building a culture of information security within your organization.
- **Subject access request policy**—organizations in regular receipt of subject access requests should consider establishing a policy on how to respond to particular requests to ensure consistent practice. If there are practical limits to data subjects' rights engendered by the architecture of the data, or you seek to rely on exemptions that would limit those rights because compliance would prejudice, prevent or seriously impair you from processing personal data that is required or necessary for your purpose, then you should document and justify the basis for doing do. Whereas all subject access requests must be treated on merit on a case-by-case basis, if you know that you are unable to comply with certain requests because you have for example stripped key identifiers from a dataset, then it is good practice to state this in your information notices and data processing statements. You should log all subject access requests, your responses to them, and any justification for refusing to comply in case the data subject seeks redress from a supervisory authority or court.

Annex 2 – Copy of Survey Questions

ORGANIZATION DETAILS

1. Organization type

a. predominantly grant-seeking/fundraising
b. predominantly grant-making
c. predominantly advocacy
d. Other

2. Focus of work

a. Human Rights
b. Political/social change
c. Education
d. Health
e. Media
f. Environment
g. Other

3. Size of organization (employees)

a. 1-10
b. 10 - 25
c. 25 - 50
d. 50 - 100
e. 100 - 250
f. 250+

4. Annual budget (Euros)

a. 0-100K
b. 100-250K
c. 250-500K
d. 500-1 million
e. 1 million +

5. Headquarters' location

- Drop down list of countries

6. Scope of activities

a. National
b. European
c. International

COMPLIANCE EFFORTS

1. Have you made efforts to comply with GDPR

a. Yes
b. No

2. If Y when did you start?

a. After GDPR was published (in/before April 2016)
b. Early 2017
c. Late 2017
d. Early 2018
e. Just before the deadline (May 25, 2018)
f. No compliance efforts made

3. If you made efforts to comply with GDPR, did you do any of the following

a. Published or revised privacy policy/statement
b. Published or revised cookie policy
c. Mailing list – reconsented / reviewed / deleted mailing list subscribers
d. Adopted or revised internal policies
e. Adopted or revised staff rules
f. Adopted or revised agreements with partners / processors
g. Produced or updated inventory of processing operations
h. Reviewed or changed fundraising procedures
i. Reviewed or changed grant-making procedures
j. Reviewed or changed advocacy procedures
k. Reviewed or change research procedures
l. Conducted risk assessment
m. Conducted DPIA
n. Implemented new IT systems
o. Enhanced information security
p. Deleted data
q. Reviewed or changed data retention policies
r. Designated a DPO
s. Designated a privacy officer or other dedicated staff member
t. Revised or introduced data breach policy
u. Staff awareness
v. Data protection training
w. Other

4. How much time in total do you estimate your organization has spent on GDPR compliance?

a. < 1 month
b. 1 - 3 months
c. 3 - 6 months
d. 6 - 12 months
e. 12+ months

5. Have the compliance efforts you've made had a financial impact on your organization? If yes please estimate the cost (in Euros).

a. Negligible
b. 1 - 10k
c. 10 - 25k
d. 25 - 50k
e. 50 - 100k
f. 100k+

PERCEPTION

1. **What is your perception of the GDPR in terms of the obligations it imposes on your organization**
   - Scale 1-10 (1 perfectly reasonable, 5 neutral, 10 too onerous)
2. **What kind of impact have your compliance efforts had on your organization (please add comments)**
   - Scale 1-10 (1 negative, 5 neutral, 10 positive)
3. **Across your organization as a whole, to what extent has there been buy-in that GDPR compliance policies are important?**
   - Scale 1-10 (1 minimal, 5 moderate, 10 comprehensive)
4. **To what extent has the organization's leadership been involved in advocating for the important of GDPR compliance?**
   - Scale 1-10 (1 minimal, 5 moderate, 10 comprehensive)
5. **Please comment on the impact of your compliance efforts on your organization (free text response)**

ADVICE

1. **How do you feel about the quality of publicly available advice available to help your organization comply with the GDPR?**
   a. Scale 1-10 (1 poor, 5 neutral, 10 excellent)
   b. Other comments (free text response)
2. **How do you rate the advice provided by your national regulatory authority in terms of its relevance and helpfulness?**
   a. Scale 1-10 (1 poor, 5 neutral, 10 excellent)
   b. Other comments (free text response)
3. **Have you had to seek external data protection advice, if so who did you contact?**
   a. Regulatory authority
   b. Lawyers
   c. Consultants
   d. Other NGO
   e. Charity regulator
   f. Umbrella group
   g. No external advice sought
   h. Other
4. **Is there any advice you found particularly helpful, if so please specify or provide a link here (free text response)**

SELF ASSESSMENT

1. **How do you feel that your organization is placed in terms of its compliance status at present?**
   - Scale 1-10 (1 concerned about compliance, 5 neutral, 10 confident)
2. **How do you feel that your organization is placed in terms of its understanding/awareness/familiarity with GDPR?**
   - Scale 1-10 (1 poorly-informed, 5 neutral, 10 very well informed)
3. **Do you feel that your organization has taken a relaxed or cautious/conservative approach to compliance?**
   - Scale 1-10 (1 relaxed, 5 neutral, 10 overly-cautious)
4. **How would you categorize your compliance efforts**
   a. Ad-hoc
   b. Checklist-based
   c. Risk-based and proportionate
   d. Comprehensive
   e. Overly cautious
   f. Other

COMPLIANCE ISSUES

1. **Have you struggled with any of the following issues?**
   a. Mapping and making an inventory of personal data processing activities
   b. Legal basis for processing
   c. Obtaining and recording consent
   d. Maintenance/operation of mailing lists
   e. Retention periods
   f. Information security
   g. Determining what qualifies as personal data
   h. Developing technical solutions to satisfy data subject requests (e.g. deletion or access)
   i. Other
2. **Please elaborate on the compliance issues encountered (free text response)**

Has your organization adopted a procedure for responding to subject access requests?

   a. Yes
   b. No

3. **Has your organization received any subject access requests?**
   a. Yes – from employees past or present
   b. Yes – from mailing list subscribers
   c. Yes – from people you are investigating
   d. Yes – from the police
   e. No
   f. Other
4. **What did the requests concern**
   a. Access
   b. Correction
   c. Deletion
   d. Erasure/right to be forgotten

e. N/A

f. Other

5. Do you consider any of the subject access requests you have been to be "vexatious", i.e. maliciously made in order to inconvenience your organization or get access to information that should otherwise be confidential?

a. Yes

b. No

6. Please provide further details about the vexatious subject access request (without including any personal details about the data subject)

7. Have you had to seek external advice as to how respond to subject access requests?

a. Yes

b. No

DATA SECURITY

1. Do you have an organizational data security policy

a. Yes

b. No

2. How concerned are you about government surveillance?

- Scale 1-10 (1 not concerned, 5 neutral, 10 extremely worried)

3. How concerned are you about other forms of unauthorized access/hacking etc?

- Scale 1-10 (1 not concerned, 5 neutral, 10 extremely worried)

4. How concerned are you about the protection of personal data related to partners/collaborators/information sources?

- Scale 1-10 (1 not concerned, 5 neutral, 10 extremely worried)

5. Do you have any other data security concerns? (free text response)

6. Have the steps you have taken to address concerns about information security changed because of the GDPR?

a. Yes

b. No

c. N/A

7. Has your organization ever experienced a personal data breach?

a. Yes

b. No

8. If yes, please provide details on the data breach (excluding any information the could compromise your organization)

GDPR'S IMPACT ON YOUR CORE ACTIVITIES

ADVOCACY

1. If your organization engages in advocacy, has the GDPR impacted any of the following practices?

a. Outreach to supporters

b. Outreach to policy-makers

c. Use of traditional media (phone, postal, email)

d. Use of social media

e. Retention of data

f. N/A

g. Other

2. What effect has GDPR had on your organization's advocacy work?

- Scale 1-10 (1 detrimental, 5 neutral, 10 positive)

RESEARCH

3. If your organization engages in research and documentation has the GDPR impacted any of the following practices?

a. Collection of personal data related to human rights violations

b. Collection of personal data related to abuse of power

c. Collection of personal data related to corruption

d. Collection of personal data related to investigative journalism and reporting

e. Collection of personal data related to public opinion (surveys etc)

f. N/A

g. Other

4. What effect has GDPR had on your organization's research work?

- Scale 1-10 (1 detrimental, 5 neutral, 10 very positive)

5. Please add any other comments about the effect of the GDPR on your organization's investigation, research and documentation work (free text response)

FUNDRAISING PRACTICES

6. If your organization engages in fundraising from the public has the GDPR impacted any of the following practices?

a. Communication with individual donors

b. Donor mailing list

c. Management of payments

d. Use of third party fundraisers

e. N/A

f. Other

7. What effect overall has GDPR had on your organization's fundraising work?

- Scale 1- 10 (1 detrimental, 5 neutral, 10 very positive)

8. Please add any other comments about the effect of GDPR on your organization's fundraising work (free text response)

GRANT-MAKING

9. If your organization engages in grant-making has the GDPR impacted any of the following practices?

a. Communications with applicants and grantees
b. Application procedures
c. Retention of application/grantee data
d. Use of application/grantee data
e. N/A
f. Other

10. What effect overall has GDPR had on your organization's grant making work?

- Scale 1-10 (1 detrimental, 5 neutral, 10 very positive)

11. Please add any other comments about the effect of GDPR on your organization's grant making work (free text response)

ENFORCEMENT

12. Has your organization been the subject of enforcement action by a regulatory authority for an alleged violation of GDPR or data protection laws?

a. Yes
b. No

13. If yes, please describe what happened (free text response)

14. Do you know of any another non-profit organizations that have been the subject of enforcement action by a regulatory authority for an alleged violation of GDPR or data protection laws?

a. Yes
b. No

15. If yes and the information is in the public domain please provide further details (free text response)

a. Beyond the GDPR
b. National law

16. Does national data protection law require you to register as a Data Controller?

a. Yes
b. No

17. Does your national law introduce additional data protection compliance obligations?

a. Yes
b. No

18. If yes please provide further details (free text response)

RELATIONSHIP WITH OTHER LEGAL REQUIREMENTS

19. Have you encountered tensions between GDPR and other regulatory requirements that apply to your organization?

a. Yes
b. No

20. If yes what do these relate to?

a. Licensing/registration
b. AML/CFT rules
c. Beneficial ownership
d. Transparency requirements
e. N/A
f. Other

ANY OTHER COMMENTS

21. Please provide any other information about your organization's experience with GDPR

Annex 3—Guidance and reference documents consulted

EUROPEAN CENTRE FOR NOT-FOR-PROFIT LAW

Data Protection Standards for Civil Society Organisations, Carly Nyst 2018.

Issues Addressed: CSO fundraising

- Overview of international data protection legal framework;
- Interaction of data protection with other legal frameworks including anti-money laundering and counterterrorism financing obligations;
- Impact of GDPR on CSO fundraising initiatives;
- Findings/recommendations:
  - Data protection laws may curtail some CSO fundraising activities because individuals' consent may be required (e.g. wealth screening);
  - CSOs of all types must comply with the data protection requirements applicable to them, including GDPR;
  - Smaller CSOs may struggle to meet onerous compliance obligations;
  - CSO specific guidance should be issued to provide support and certainty to CSOs about their GDPR and data protection obligations;
  - Domestic legislation (including laws around charity fundraising, data protection, cyber crime and national security) must be consistent with and reflect international human rights law.

INFORMATION COMMISSIONER'S OFFICE (ICO)

Resources for charities

Issues Addressed: Resources for charities

- ICO Charity GDPR page provides resources, links, responses to FAQs.
- A GDPR self assessment toolkit is available to help organisations generally determine their compliance status.
- No charity specific GDPR guidance has been issued by ICO (general guidance has been issued as outlined below), but ICO advise that they are engaging with representatives from the charity sector to assist them in producing their own sector specific guidance.
- A helpline was opened to allow small organisations to contact ICO and get advice directly.

GDPR FAQs for charities

Issues Addressed: How to deal with health data, consent and appointing a DPO for charities

- Key points:
  - All charities, regardless of size, must comply with the law, including GDPR.
  - Health data, which is sensitive personal data under the DPA, will come under the definition of special category data under the GDPR.
  - Consent for marketing obtained prior to the effective date of GDPR should be reviewed to ensure that it meets the GDPR standard and can continue to be relied upon. Where existing consent do not meet the GDPR standard or are poorly documented, then that consent should be refreshed, a different lawful basis should be identified or the processing should be stopped.
  - Consent is not the only lawful basis that can be relied upon for marketing under GDPR but it is required for some calls, texts and emails under the Privacy and Electronic Communications Regulations 2003 (PECR).
  - Any organisation is able to appoint a DPO. Public authorities and organisations whose core activities include large scale systematic monitoring of individuals, and/or relate to large scale processing of special categories of data or data related to criminal convictions or offences. Regardless of whether a DPO is required under GPDR, all organisations must ensure they have sufficient staff and skills to adhere to the obligations under GDPR.

Transcript of speech delivered by the Information Commissioner to the Fundraising and Regulatory Compliance Conference in February 2017

Issues Addressed: Charity fundraising

- Addresses compliance with the then current Data Protection Act (DPA) 1998 and how to prepare for the GDPR, primarily in response to the findings produced from ICO investigations into a number of charitable organisations' fundraising practices.
- The investigations uncovered serious breaches of the DPA 1998 related to wealth screening without individuals' consent (the practice of tracing and targeting individuals by bringing together personal information from numerous sources, some charities were also trading personal details with other charities, creating a large pool of donor data for sale).
- While the activity of wealth screening was not explicitly prohibited by the law, the practice contravenes the fundamental principles of data protection laws when done without the consent of the individuals affected.
- Data protection is a matter for the boardroom, not to be dealt with in isolation by one or more parts of a charity (e.g. IT or fundraising).
- Public information is not "fair game", once it comes into the hands of a charity, that data must be treated fairly and in line with the law, which includes treating the data in a way that people would expect.
- Profiling and wealth screening is not something that people would expect to happen to them without their knowledge or consent.
- Consent must be freely given, informed and unambiguous and you must be able to prove you have it if you rely on it for processing. A pre-ticked box will not be valid consent.

Conference presentation and conference paper

Issues Addressed: Charity fundraising

- Focused on considerations for charities regarding the use of publicly available data, wealth screening, data matching and tele-appealing.
- Addresses consent, legitimate interests and fairness and transparency of processing under DPA 1998.
- The use of publicly available information is still subject to proper treatment under data protection laws regardless of how it was obtained.
- Consideration of the data protection implications of wealth screening, data matching and teleappealing

Findings from ICO information risk reviews at eight charities

Issues Addressed: Data management review of eight UK charities

- In April 2018, ICO published findings from its review of eight charities highlighting the effectiveness of the controls in place to safely manage data, and to what extent these practices were embedded. The report sets out areas of good practice and areas for improvement, including governance; policies and procedures; monitoring and reporting; training; consent; fair processing and data sharing; business continuity; incident reporting and retention and disposal.

ICO Guide to the GDPR

Issues Addressed: General compliance guide

- ICO GDPR general compliance guide

INTERNATIONAL COMMITTEE OF THE RED CROSS

Handbook of Data Protection in Humanitarian Action

Issues Addressed: Compliance guide specific to humanitarian actors in emergency situations

- Guidance on data protection principles as applicable to humanitarian emergencies;
- Provides specific guidance on the interpretation of data protection principles in the context of humanitarian action, particularly where new technologies are employed.

FUNDRAISING REGULATOR (FR)

Regulatory guidance and resources

Issues Addressed: Charity fundraising

- FR has produced briefing notes which cover GDPR compliance matters specific to fundraising for:
  - Corporate entities;
  - Legacies;
  - Community groups;
  - Charitable trusts;
  - As well as a general introduction to GDPR.
- These notes relate specifically to how GDPR impacts fundraising activities, particularly around contacting individuals for donations, covering matters including:
  - direct marketing under GDPR;
  - an explanation of the consent and legitimate interest lawful bases;
  - the lawful basis that may be relied upon for different types of communication when reaching out to individuals for fundraising purposes;
  - the content of privacy notices
  - some information about the interaction between GDPR and the Privacy and Electronics Communication Regulation 2013 (PECR).

Personal information and fundraising resources

Issues Addressed: Charity fundraising

- Personal information and fundraising: consent, purpose and transparency
  - focus on direct marketing and communication for the purpose of fundraising in the context of data protection laws;
  - establishing a lawful basis for different types of communication (email, SMS, automated calls, fax, live calls and post);
  - opt-in/opt-out consent under GDPR;
  - fairness and transparency requirements under GDPR;
  - advice on using third party data suppliers (fundraising platform providers, buying personal data and data collection) and where a third party supplier uses charity data to provide a service for the charity.
- Consent case studies from eight charities who have reconsidered their approach to donor consent since 2016
  - case studies detailing the approach by eight charities to managing their existing mailing list and changing their approach to opting new individuals in, in line with the requirements of GDPR, covering "consent refreshing" and other approaches from Age UK, Cancer Research UK, Macmillan Cancer Support, Rethink Mental Illness, RNLI, Rose Road Association, RSPCA and The Children's Society.
- Consent self-assessment tool
- Checklist for charities using consent

INSTITUTE OF FUNDRAISING

Connecting people to causes: a practical guide to fundraising research

Issues Addressed: Fundraising guidance for charities

- Guidance for charities on using and collecting personal data from individuals who they wish to target for the purposes of fundraising, including publicly available information.
- "GDPR is principles-based, rather than directly prescriptive", the document aims to provide an outline of the process to go through to help guide organisations' use of personal data in fundraising work.

GDPR resources

Issues Addressed: Resources for fundraisers

- Resources and advice for charities especially around GDPR and direct marketing, which includes fundraising activities.

DIRECT MARKETING ASSOCIATION

GDPR Checklist

Issues Addressed: Guidance for managing personal data for direct marketing purposes (applicable to advocacy)

- Applies to direct marketing activities, including fundraising;
- Covers legitimate interests, consent, the kind of information that needs to be supplied to data subjects, the use of data sourced from third parties, profiling and legacy data.

NATIONAL COUNCIL FOR VOLUNTARY ORGANISATIONS (NCVO), INCLUDING THE KNOW HOW NON-PROFIT RESOURCES

GDPR webinar

Issues Addressed: General compliance advice for voluntary organisations

- Covers data protection principles;
- Organisational structure and steps to take toward compliance;
- Lawful bases;
- Appointment of a DPO;
- Includes interactive responses from organisations to gauge preparedness/compliance status;
- Q&A session at end covering:
  - Consent – what level of granularity required? Separate consents for separate processing operations required under GDPR, but question is how to separate out those operations?
  - Fundraising Regulators guidance says that separating out the activities of the organisation should guide how to separate consent for contacting individuals, e.g. an organisation may undertake research, fundraising, advocacy campaigning, running events = a number of different activities that individuals may or may not want to participate in or be contacted about, so consent to contact about these different activities must be separated out. Where an organisation chooses not to separate out consent in these circumstances, they need to be confident about why they are making this decision and be able to support this and consider that withdrawal of the consent would impact contact about all of these different processes.
  - Records of consent must be kept. Where the consent relates to sensitive personal data, a strong record of agreement should be created (e.g. a more detailed consent form requiring electronic signature). For less sensitive information, a record of an unambiguous consent may suffice (e.g. a tick box).
  - Evidence for consent received verbally e.g. over the phone - guidance from ICO (in draft at the time of the session) is clear about being able to demonstrate back to the person what they agreed to. If it is verbal, is there a set statement that was read to the individual and they agreed? Having a script or clarity of this kind on record is essential. For more sensitive data a recording of the consent may be required.
  - Many ways to obtain GDPR standard consent when it comes to non-sensitive personal information.
  - When should consent be sought? Do clients and volunteers need to opt-in to receive contact about organisational events? For organisational information critical to the role of the client/volunteer/operations of the organisation, there is a legitimate interest in communicating this without asking for consent. For communication about non-mission critical information (e.g. invitations to social/other events) these should be sent on an opt-in basis as it is reasonable to provide individuals with a choice about receiving these.
  - Understand what messages NEED to be communicated vs circumstances where individuals might reasonably be given a choice about receiving messages.
  - DPO – to whom should a DPO report? Senior management within the organisation, for charities that is trustee level (they can make decisions about allocating budget and resource and the management of information in the organisation).

Data Protection and GDPR, Know How Non Profit

Issues Addressed: Resources for non-profits

- Links and resources to GDPR compliance guidance material from ICO;
- Guidance on how to write privacy policies and sample policies;
- Access to a GDPR compliance "health check" review service by NCVO consultants.
- How to Comply with GDPR, Know How Non Profit
- General compliance advice
  - Advice to non-profits:
  - Ensure trustee board and senior staff are aware of the organisation's compliance obligations;
  - Identify data held and its source,
  - Update privacy notices in compliance with GDPR;
  - Review processing activities against individual's rights, e.g. right to deletion/correction of data;
  - Put a plan in place for dealing with subject access requests;
  - Identify processing activities and their lawful basis;
  - Review consent practices;
  - Build in extra protections for children where relevant;
  - Put a plan in place to detect, report and investigate personal data breaches;
  - Ensure fundraising practices are compliant.

EUROPEAN COMMISSION ARTICLE 29 WORKING PARTY

Article 29 Guidelines

Issues Addressed: Detailed guidance on the application of particular principles of GPDR

Transparency

- Provides practical guidance and interpretative assistance on the new obligation of transparency concerning the processing of personal data under the GDPR.
- Transparency is an overarching obligation under the GDPR applying to three central areas:
  - (1) the provision of information to data subjects related to fair processing;
  - (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and
  - (3) how data controllers facilitate the exercise by data subjects of their rights.
- These guidelines are, like all WP29 guidelines, intended to be generally applicable and relevant to controllers irrespective of the sectoral, industry or regulatory specifications particular to any given data controller.

Automated individual decision-making and Profiling

- Definitions of profiling and automated decision-making and the GDPR approach to these in general – Chapter II;
- General provisions on profiling and automated decision-making – Chapter III;
- Specific provisions on solely automated decision-making defined in Article 22 - Chapter IV;
- Children and profiling – Chapter V;
- Data protection impact assessments and data protection officers– Chapter VI;
- Best practice recommendations, building on the experience gained in EU Member States.

Personal data breach notification

- Explanation of the circumstances in which a personal data breach is to be notified to a national supervisory authority or lead authority, and communicated to the individuals whose personal data have been affected.

Consent

- Thorough analysis of the notion of consent.
- The concept of consent as used in the Data Protection Directive and in the e-Privacy Directive to date, has evolved.
- The GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent.
- These Guidelines focus on these changes, providing practical guidance to ensure compliance with the GDPR and building upon Opinion 15/2011 on consent.
- The obligation is on controllers to innovate to find new solutions that operate within the parameters of the law and better support the protection of personal data and the interests of data subjects.

Application and setting of administrative fines

- This document is intended for use by the supervisory authorities to ensure better application and enforcement of the GDPR and expresses their understanding of the provisions of article 83 as well as its interplay with articles 58 and 70 and their corresponding recitals.
- In particular, according to article 70, (1) (e), the European Data Protection Board is empowered to issue guidelines, recommendations and best practices in order to encourage consistent application of the GDPR and the setting and application of administrative fines.

Lead Supervisory Authority

- Explains in what circumstances the LSA principle is relevant and applicable, i.e. where a controller or processor engages in cross-border processing of personal data, the LSA is the authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data.

Data Protection Officers (DPO)

- Explains the role of the DPO and in what circumstances a DPO should and/or must be appointed.

Data Portability

- Explanation of the right to data portability and how it can be given effect by data controllers.
- Data subjects have the right to receive the personal data that they have provided to a data controller in a structured, commonly used and machine-readable format that can be transmitted to another data controller without hindrance.

Guidelines on Data Protection Impact Assessment (DPIA)

- The purpose of this document is to clarify the relevant provisions of the GDPR in order to help controllers to comply with the law and to provide legal certainty for controllers who are required to carry out a DPIA. These Guidelines also seek to promote the development of:
  - a common European Union list of processing operations for which a DPIA is mandatory (Article 35(4));
  - a common EU list of processing operations for which a DPIA is not necessary (Article 35(5));
  - common criteria on the methodology for carrying out a DPIA (Article 35(5));
  - common criteria for specifying when the supervisory authority shall be consulted (Article 36(1));
  - recommendations, where possible, building on the experience gained in EU Member States.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL HUMAN RIGHTS (FRA)

Handbook on European data protection law 2018

Issues Addressed: General compliance advice for legal practitioners

- Handbook designed to familiarise legal practitioners not specialised in data protection with this emerging area of the law.

Information society, privacy and data protection

Issues Addressed: Compliance advice and information on data protection generally.

- FRA's work on information society, privacy and data protection (including links to all relevant FRA reports).

CHARITY FINANCE GROUP

GDPR: A guide for charities

Issues Addressed: General compliance advice for charities

- Advice on governance, fundraising, financial data, beneficiary data, employee data

CONCORD

What does GDPR mean for your organisation?

Issues Addressed: Webinar presentation for relief and development NGOs

- Concord attended several GDPR conferences, exchanged information with some Concord members and peers and consulted a lawyer who helped them to order their compliance process and give them the framework to develop the tools they require to be complaint.
- With this information Concord organized a webinar open to members and partners in which they share what they had learnt and the compliance steps they had taken.

UNITED NATIONS

Data, privacy, ethics and protection guidance note on big data for achievement of the 2030 agenda

Issues Addressed: Guidance document setting out general guidance on data privacy, protection and data ethics for the United Nations Development Group

- The guidance sets out principles for obtaining, retaining, using and quality controlling data from the private sector

Annex 4—Data processing inventory template

Dataset	Owner	Data processed	Purpose	Legal basis	Risk level	Storage	Status	Access	Data sharing with third parties	Policies / notices required
Individual donors	Fundraising lead	Name, email address, amount donated, frequency	Fundraising	Consent (initial contact), legitimate interest (follow up contact with individuals who have donated)	Medium	Organization server	Active	Fundraising team	n/a	Information notice to obtain consent from data subjects
Subscriber mailing list	Director, Community Developer	Name, email address	Reaching out to and informing network of ongoing work and upcoming events	Consent	Low	Organization server, email service provider platform	Active	Community Development Team	Email service provider platform	Information notice to obtain consent from data subjects.
Staff travel booking	HR	Staff name, personal contact details, copies of passports.	Arranging staff	Compliance with a legal obligation (information required to book travel) and contract (condition of employment that this information will be processed)	High	Organization server, travel booking platform and websites	Active	HR	Travel booking platform and websites	Clause within employment contract that explains how staff data will be processed for this purpose.

OPEN SOCIETY
FOUNDATIONS