DATA PROTECTION STANDARDS FOR CIVIL SOCIETY ORGANISATIONS

Author: Carly Nyst

This report is wholly financed by the Swedish International Development Cooperation Agency (Sida). Sida does not necessarily share the opinions here within expressed. The author bears the sole responsibility for the content.

This study was conducted as part of the 'Sustainable Frameworks for Public Fundraising: research and guidance' project, managed by the European Center for Not-for-Profit Law (ECNL). The project is made possible by the International Center for Not-for-Profit Law (ICNL) through the Civic Space Initiative.

Table of content

I. Introduction and background

A. About this paper

In November 2017, the European Center for Not-for-Profit Law (ECNL), along with the International Center for Not-for-Profit Law (ICNL), published a comparative research report on the regulatory framework for fundraising in Europe. The research maps out a spectrum of issues that affect the right of civil society organisations ("CSOs") to secure resources, and identifies a series of regulatory and policy challenges affecting both cross-border and domestic fundraising activities of CSOs, including data protection and privacy regulation.

With the objective of expanding upon its existing research and ultimately creating guidelines on international regulatory standards on fundraising and toolkits to help local stakeholders assess the current health of the environment for fundraising in their countries, ECNL commissioned this research paper, authored by Carly Nyst, on privacy and data protection policy and law**. The paper aims to identify how the right to privacy interacts with CSOs' right to fundraise, and provide general guidance as to the application of data protection standards to CSOs' fundraising initiatives.** By canvassing existing international, regional and domestic data protection and privacy laws and policies, this paper explains at a high level the ramifications of data protection standards for CSOs, with a particular focus on how data protection standards may protect or constrain CSOs' right to fundraise. The paper specifically addresses the consequences of the European Union's General Data Protection Regulation, which comes into force in May 2018, for CSOs. It concludes by making recommendations about how to reconcile fundraising activities with data protection, with targeted suggestions for CSOs and policy makers to this end.

B. The origins and history of data protection law

The **right to privacy is a fundamental human right**, enshrined in a number of international human rights instruments, including the Universal Declaration of Human Rights.[1] More than 150 constitutions around the world contain provisions related to privacy in its various forms.[2]

The right to privacy requires that all individuals should be free from arbitrary or unlawful interference with their privacy, home, correspondence and family, and from attacks upon their reputation. In tangible terms, **the right to privacy protects**:

- the confidentiality of letters, phone calls, emails, text messages and internet browsing;
- the sanctity of the home;
- the ability of individuals to make decisions about their lives, including about their sexual and reproductive choices; and
- individuals' control of their personal data.

Privacy is closely tied to, and underpins, the concept of human dignity, which ensures that individuals are empowered to make autonomous decisions about their lives without interference from the State, or from private actors. Privacy is also an important enabling right, providing the conditions for individuals to enjoy other human rights, such as the right to freedom of expression, association and peaceful assembly.

As technology has advanced, the right to privacy has evolved to encompass a right to the protection of personal data. Advancements in computing power have made it possible to generate, collect and retain vast amounts of data, and has permitted previously unimaginable forms of data. The internet and the use of digital communications have dramatically expanded the opportunities for personal data to be shared and accessed, including by unauthorised actors. Protecting privacy is no longer a matter of sealing an envelope or locking a door; it requires strict technical and organisational practices undertaken within a legal framework.

[1] See, for example, the Universal Declaration on Human Rights, Art. 12; the International Covenant on Civil and Political Rights, Art. 17; the European Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 8; and the American Convention on Human Rights, Art. 11.

[2] See the Constitute project: https://www.constituteproject.org/search?lang=en&key=privacy.

As early as 1989 the United Nations recognised that the collection and use of personal data must be regulated by law.[3] Since that time, **a body of law has developed that elaborates upon the right to privacy in the context of the use of personal data; this is known as "data protection law."**

Three international texts provide the groundwork for modern day data protection law:

- The **1980 Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**, the first international statement on the specific conditions under which personal information should be handled in order to ensure an individual's right to privacy is respected;
- The **Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (known as Convention 108), the first internationally binding instrument on the protection of personal information;[4]
- Enshrining the principles of the OECD Guidelines and Convention 108, the **European Data Protection Directive** 95/46/EC, adopted in 1995, became a leading standard for data protection law around the world. There are more than 100 national data privacy laws around the world, nearly half of which are from outside Europe,[5] and many of these laws closely mimic the European Directive.

C. A new generation of data protection

The coming years will see a new generation of data protection laws across the world. Indeed, it is possible that **we are entering a new era of understanding about the importance of privacy and the protection of personal data,** one which may catalyse significant changes not only to laws but to technologies, corporate practices and financial models.

[3] ICCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, para. 10.

[4] The Convention has been signed by all 48 Council of Europe members and ratified by all but Turkey; in addition, Uruguay, Mauritius and Senegal have all ratified the Convention. In 2001, Convention 108 was supplemented with an Additional Protocol regarding the Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows" (the Additional Protocol).

[5] Graham Greenleaf, Asian Data Privacy Laws (Oxford, Oxford University Press: 2014), 55. For details about each of the domestic frameworks, see BakerHostetler, 2015 International Compendium of Data Privacy Laws, available at http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf

This fundamental shift will begin in Europe where, **in May 2018, the General Data Protection Regulation ("the GDPR") will replace the Data Protection Directive**, and will considerably strengthen and upgrade data protection in Europe. Although it rests on the same fundamental principles as the Directive before it, the GDPR expands individuals' rights, extends the role and enforcement powers of data protection authorities (independent national supervisory authorities charged with monitoring compliance and investigating breaches), and places a stronger burden on data controllers (the entities who collect and process personal data) to be transparent and accountable to individual data subjects. It also broadens the definition of personal data to include "online identifiers", and expands the category of sensitive data (now called "special categories of data") to include biometric and genetic data. **Some of the major changes that the GDPR makes to individuals' rights are summarised in the table below.**

GDPR changes to data protection principles and rights

EU Data Protection Directive	General Data Protection Regulation
Personal data to be processed fairly and lawfully. If consent is the lawful basis for processing, it must be unambiguously given.	Personal data to be processed lawfully, fairly and in a transparent manner in relation to the data subject [Art. 5(1)(a)]. If consent is the lawful basis for processing, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent [Art. 7]. Silence, pre-ticked boxes or inactivity should not therefore constitute consent [Recital 32].
Data processors and controllers to adopt appropriate technical and organisations measures.	Data processors and controllers must take technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia, as appropriate, the pseudonymisation and encryption of personal data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons [Art. 32(1)].
Information to be given to data subject about the use of their personal data	Data controllers must, at the time at which personal data are obtained [Art. 13], provide the data subject with information about the identity of the controller and its data protection officer, the purposes for the processing, the legitimate interests pursued (if applicable), the recipients of the data, the period for which it will be stored, and the rights of the data subject, whether or not the data is collected directly from the data

	subject [Art. 14]. The controller shall take appropriate measures to provide that information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child [Art. 12]
Individuals have the right to access and correct personal data, and to erasure under certain circumstances.	Individuals have the right to: access their personal data [Art. 15], rectify or complete their personal data [Art. 16], erasure ('right to be forgotten') [Art. 17], restriction of processing [Art. 18] and data portability [Art. 20]. Data controllers have an obligation to notify all recipients of data of requests to rectify or erase data or restrict processing [Art. 19].
Individuals have the right to object to processing under certain circumstances	Individuals have the right to object to processing under certain circumstances [Art. 12]
Individuals have the right not to be subject to some automated individual decisions	Individuals have the right not to be subject to automated individual decisions which produce legal effects [Art. 22]

Beyond the GDPR, the European Union has signalled its intention to more broadly regulate the acquisition and use of personal data, particularly in the context of large internet companies and digital technologies. For example, the existing Privacy and Electronic Communications Directive 2002/58/EC (also known as the ePrivacy Directive) is currently undergoing review with a view to the adoption of an ePrivacy Regulation in 2018. If adopted in its current form, the ePrivacy Regulation will even further strengthen obligations on entities, including CSOs, regarding direct marketing. Under the existing Directive entities must obtain consent from individuals before sending them marketing materials by email, text or phone. The Regulation will require that consent adheres to the same standards as those required by the GDPR, including that it must be freely given, specific, informed and unambiguous, and that it must not include silence, pre-ticked boxes or inactivity. The Regulation will also specify that the same requirements apply to a broader range of technologies, like instant messaging services and in-app notifications.

These EU reforms are likely to have global consequences. Because of data transfer requirements in the GDPR (just as there were in the Data Protection Directive), countries outside the European Union are incentivised to adopt equivalent protections in order to create a commercial environment which is

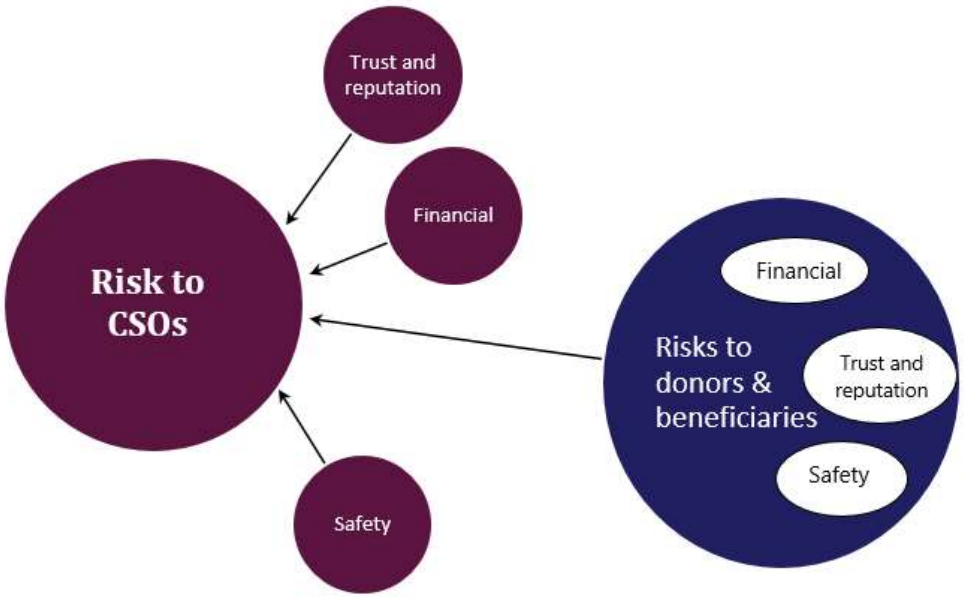
hospitable to data transfers and business process outsourcing.[6] In recent years, countries such as the Philippines have undergone major legislative reform to ensure that domestic regulatory frameworks mimic the existing EU legislation. The "trickle down" effect of EU data protection law also emerges because the effect of the law is to regulate not only the activities of EU entities, but of all entities that process EU citizens' data (including CSOs). Specifically, the GDPR applies to organisations established outside of the EU when those organisations offer goods or services to individuals in the EU, or where organisations monitor the behaviour of individuals within the EU. In practice, this means that organisations often choose to apply the higher EU protections worldwide, to facilitate and simplify compliance. In the case of CSOs outside of the EU, consideration will need to be given to compliance with the GDPR where CSOs target EU residents for fundraising, for example, or where CSOs deliver assistance to beneficiaries based in the EU.

D. The value of data protection for civil society organisations

The risks that arise through the collection and storage of personal data are neither remote nor theoretical. Organisations that are lax or negligent with how they collect, use and store personal data not only create risks for themselves – the reputational risk of being exposed by the media or fined by a regulator, the financial risk of having to meet punitive fines or losing data to online criminals, and the loss of trust by donors and supporters – but for the individuals whose data they process. That includes the personal data of donors and supporters on whom the organisation relies, the personal data of employees and volunteers, and the personal data of beneficiaries, whose data may be particularly sensitive and who may be some of the most vulnerable people in society. **The data that many CSOs hold may be of interest to any number of malevolent actors, including non-state actors, governments and commercial interests.** Even the most seemingly benign data deserves protection because of the flow on effects that its loss, misuse or theft might cause for the individuals to whom it pertains.

[6] Indeed, the EU is actively promoting the adoption of data protection legislation which conforms to the GDPR in countries outside the EU, in order to promote harmonisation of regulation for the business community.

Risks of non-compliance with data protection standards



Civil society organisations around the world are increasingly learning the value of data protection and realising the ethical and legal imperatives to adopt strong data protection policies and processes. A particularly impressive example is that of Oxfam, which has invested heavily in the responsible management and use of programmatic data.[7] Oxfam has placed five "responsible data" principles at the heard of its programme work: the right to be counted and heard, the right to dignity and respect, the right to make an informed decision, the right to privacy, and the right not to be put at risk. In 2015, Oxfam self-imposed a moratorium on adopting new technologies like biometrics, out of concern that early adoption of new technologies without a proper assessment of the risks to data protection might result in harm to beneficiaries. In doing so, Oxfam has explicitly recognised that data protection is not just an issue of compliance or technical security, but rather about putting human rights at the heart of all its work.

As a large international non-governmental organisation, Oxfam admittedly has more resources to draw upon to mainstream data protection. Yet it also has more points of vulnerability and faces greater challenges in implementing and enforcing policies than smaller organisations. It operates programmes across countries and jurisdictions, often in contexts with weak legal institutions and poor telecommunications infrastructure. It also works in hostile environments where governments and non-

[7] Oxfam Responsible Program Data Policy, 17 February 2015.

state actors might specifically seek access to the personal data Oxfam holds, requiring far more investment in information security protocols. In any event, **a civil society organisation's size has no bearing on whether it has obligations to protect privacy and data protection**. That is a matter of international, regional and domestic law, as discussed below.

Beyond legal obligations, however, civil society organisations should be encouraged to recognise the ethical imperative underpinning ensuring personal data is protected. **Creating an internal organisational culture which appreciates the value of personal data and prioritises its protection is an important first step in this regard.** After all, CSOs also benefit from the right to privacy and data protection. For example, in some circumstances CSOs could rely on data protection law to defend against requests for information on donors or beneficiaries, or to redact financial disclosure documents. The right to privacy protects CSOs from arbitrary and unlawful surveillance, both domestic and foreign, of their communications and online activities. In order to comply with the right to privacy, State surveillance of CSOs must be lawful, necessary and proportionate, and be accompanied by specific safeguards and overseen by strong and independent authorities.[8]

Interpreting the basic principles of data protection law for CSOs

DATA PROTECTION PRINCIPLE	EXAMPLES OF CONCRETE APPLICATION FOR CSOS
Fair and lawful processing Personal data should be processed in a fair, lawful and transparent manner.	A CSO should ask an individual's consent to use their personal data (such as name, age and address), to share that data with third parties and to send the individual marketing communications. CSOs can also rely on other legal bases to use personal data, notably their "legitimate interests" in conducting direct marketing. CSOs may also disclose data to a third party where they are under a legal obligation to do so (for example on the presentation of a warrant by a government agency).
Purpose limitation Personal data should be collected for specified, explicit and legitimate purposes and not further	A CSO should tell an individual why it needs their date of birth (for example, to understand donor demographics) and must not use that data for incompatible purposes (for example, by selling that data to a credit scoring agency).

[8] United Nations Human Rights Committee, Concluding Observations on the fourth periodic report of the United States of America, 23 April 2014, p. 22 [CCPR/C/USA/CO/4].

processed in a manner that is incompatible with those purposes.	
Data minimisation Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.	A CSO shouldn't ask an individual to provide information on their political preferences in order to process their donation.
Accuracy Personal data should be accurate and, where necessary, kept up to date.	CSOs should regularly ask individuals to update their personal data and give them the opportunity to correct inaccurate data.
Storage limitation Personal data should be kept in a form that permits identification for no longer than is necessary for the purposes for which the personal data are processed.	CSOs should anonymise or pseudonymise data as soon as it is no longer necessary to keep data in identifiable form. For example, if data on past donations is being kept periods longer than that required for financial reporting and auditing, CSOs should consider removing the identifying features of the data or pseudonymising the dataset.
Security Personal data should be processed in a way that ensures their security, using appropriate technical and organizational measures.	CSOs must ensure their technical systems use up-to-date software and that payment sites guarantee encrypted transactions.
Transparency and accountability The data controller is responsible for complying with and demonstrating compliance with data protection principles.	CSOs should appoint a data protection officer or delegate this responsibility to somebody within the organization and should ensure they publish information about their data protection practices.

E. The impact of privacy and data protection standards on CSOs

Privacy and data protection obligations may have a broad range of implications for CSOs. These implications may be felt both as CSOs carry out their core functions, as well as when they conduct fundraising to support those functions.

i Carrying out core functions

CSOs may need to take privacy and data protection standards into consideration when:

- Delivering assistance to beneficiaries

Some CSOs deliver aid and assistance directly to beneficiaries, and in the process they collect and process beneficiaries' data. For example, CSOs may provide legal assistance or accommodation to newly arrived refugees and asylum seekers, and keep databases of information which are shared with prescribed public services. Sometimes that data may qualify as "sensitive" or belonging to a "special category" of personal data, such as health data or data about religious or ethnic affiliations. **In all circumstances, CSOs need to ensure that in carrying out their core functions they respect privacy and data protection standards, even if that means redesigning programmes to limit the collection of personal data.**

- Conducting research

Some CSOs use surveys, publicly available information and other datasets to conduct research in the public interest. Often datasets will contain sensitive information such as health or genetic data or information on political or religious affiliations. **In some cases, scientific, historical or statistical research will be exempt from some data protection provisions**.[9] However, CSOs cannot assume that simply because they are processing personal data for a research purpose that the processing is exempt from privacy requirements.

- Campaigning and public statements

The right to privacy encompasses the right to protection of reputation,[10] although this element of privacy remains subject to unequal protection[11] and its implementation is subject to debate. **When CSOs exercise their right to speak publicly and disseminate information,[12] this right may be tempered in light of, and balanced against, the right of individuals to have their reputation**

[9] For example, see Art. 89 of the GDPR.

[10] Art. 12, Universal Declaration of Human Rights

[11] For example, Article 8 of the European Convention of Human Rights, which otherwise mirrors Article 12 UDHR, does not explicitly reference the right to reputation, although it has been implied in the jurisprudence of the European Court of Human Rights: see Polanco Torres and Movilla Polanco v. Spain, ECHR, 21 September 2010, Application no. 34147/06.

[12] Protected by Article 19 of the Universal Declaration of Human Rights, Article 19 of the International Covenant on Civil and Political Rights, and Article 10 of the European Convention of Human Rights, amongst others.

protected against direct attacks. Numerous areas of regulation pertain to the protection of reputation, including libel law, comprising defamation actions (relating to false statements which impact upon reputation), as well as civil actions related to the protection of human dignity and the protection of personality and images, and human rights claims.

- Responding to government requests for data

Data protection standards require CSOs to protect the personal data they acquire on beneficiaries, donors and supporters. If CSOs are presented with government requests for personal data (for example, in the form of a warrant by a surveillance agency) data protection permits the disclosure of the data, provided the CSO is under a legal obligation to do so. **CSOs should not voluntarily comply with requests for data that are not backed up by a legal obligation to disclose.**

ii. The right to fundraise

CSOs will need to take privacy and data protection standards into consideration when:

- Maintaining a database of potential and existing supporters, donors and contributors

Collecting personal data and keeping it in a database engages data protection rules and CSOs must make sure they comply with specific requirements, such as obtaining consent and ensuring technical security of databases.

- Communicating with and marketing to potential and existing supporters, donors and contributors

All communications, whether they be advertising, requests for donations or supporter newsletters, which promote the aims and ideals of a CSO amounts to "direct marketing" for the purposes of data protection standards, and must comply with particular rules. The rules on electronic marketing are often even stricter than mail marketing; for example, in the EU the ePrivacy Directive applies additional requirements for electronic marketing, requiring marketing that takes place by email, SMS or automated phone calls to be based on consent of the individual.[13] Presently, many entities rely on

[13] See, for example, the UK Information Commissioner's Office, *Direct Marketing Guidance,* available at https://ico.org.uk/for-organisations/marketing/.

implied consent, meaning they notify an individual of their right to opt out of further marketing communications. However, with the coming into force of the ePrivacy Regulation (assuming it is adopted in its current form), the standard of obtaining consent will be strengthened such as silence or pre-ticked boxes will not satisfy the consent requirements.

- "Wealth screening" and prospect research, obtaining, swapping or purchasing data about potential and existing donors

Wealth screening, by which CSOs attempt to estimate a current or prospective donor's capacity to give by analysing data based on certain indicators of wealth such as real estate ownership or stock holdings, has recently gained public attention due to the issuance by the UK Information Commissioner's Office of a series of fines against eleven British CSOs participating in the practice.[14] Because wealth screening is unlikely to be something that individuals donating to CSOs expect their personal data to be used for, it is essential that CSOs comply with notice and consent guidelines regarding such processing activities.[15]

- Data matching and teleappending

Charities use tactics such as telematching (obtaining from a third party an up-to-date telephone number for an existing donor whose number is no longer correct) or teleappending (obtaining from a third party an up-to-date telephone number for an existing donor who has never given their phone number, but who hasn't objected to phone calls) to communicate with donors and supporters. The process of obtaining personal data about donors and supporters from sources other than the individual raises concerns from a privacy and data protection perspective, as it may be unfair to the individual. CSOs will often be required by data protection standards to tell individuals what other information they have obtained about them and from which source it was obtained. This is required, for example, by the GDPR.

[14] Madhumita Murgia, "UK Charities Fined after Swapping and Selling their Donor Lists," *The Financial Times,* 5 April 2017, available at https://www.ft.com/content/a0c548e8-1a1a-11e7-a266-12672483791a

[15] See Information Commissioner's Office, *Fundraising and regulatory compliance – conference paper,* 21 February 2017.

- Selling and sharing data on potential and existing supporters, donors and contributors with other CSOs or commercial entities.

CSOs will need to comply with notice and consent obligations before selling or sharing personal data with third parties.

The remainder of this paper will focus on specific data protection and privacy obligations as they relate to the right to fundraise.

How does data protection affect fundraising activities?

TYPE OF ACTIVITY	**RELEVANT DATA PROTECTION STANDARDS (BASED ON EU LAW)**
Email and text direct marketing communications to existing donors and supporters	CSOs must ask for an individual's consent to send them communications by email and text message, and should give them a way to withdraw that consent if they change their mind. Under the GDPR, consent must be freely given, specific, informed and unambiguous, and cannot be conveyed by silence or pre-ticked boxes.
Routine email and text communications to existing donors and supporters (administrative communications about a past donation, for example, that don't contain any promotional materials).	Although CSOs need a lawful basis to send such messages, they may not need the individual's consent, but rather could rely on the organisation's "legitimate interests".
Email and text communications to prospective donors and supporters	CSOs must ask for an individual's consent to send them communications by email and text message, and should give them a way to withdraw that consent if they change their mind.
Live phone calls to existing or prospective donors and supporters	It is best practice for CSOs to ask for an individual's consent to communicate them by live phone call, but CSOs may also do so on other legal bases, most notably if they believe the organisation's "legitimate interests" outweigh the data protection rights of the individual concerned. Regardless of whether such communications are based on consent or legitimate interests, CSOs should give individuals a way to withdraw their consent to future phone calls or object to phone calls based on legitimate interest.
Automated phone calls to existing donors and supporters	CSOs must ask for an individual's consent to target them with automated phone calls, and should give individuals a way to withdraw that consent if they change their mind.

Postal communications to existing and prospective donors and supporters	CSOs do not need to ask for an individual's consent, but rather can send direct marketing materials on the basis that they are in the organisation's legitimate interests.
Wealth screening of existing donors and supporters	It is best practice for CSOs to ask for an individual's consent to use their personal data for wealth screening, but CSOs may also do so on other legal bases, most notably if they believe the organisation's "legitimate interests" outweigh the data protection rights of the individual concerned. In order to rely on legitimate interests, the CSO would need to have an existing relevant and appropriate relationship with the individual concerned and that individual would need to reasonably expect that their personal data would be used for wealth screening. If CSOs rely on legitimate interests for such a practice, they will still need to inform the individual that the practice is taking place and of their right to object to wealth screening.
Wealth screening of prospective donors and supporters	In the absence of a pre-existing relationship, it is unlikely that CSOs could rely on legitimate interests as a lawful basis for wealth screening potential donors. Rather, they would need the prospective donors' consent.
Sharing data of existing donors and supporters	CSOs can rely on consent or legitimate interests, as wells lawful obligations, to share data on donors and supporters with other CSOs, third party companies or governments. Regardless, they will need to inform individuals of with which entities their personal data have been shared.
Obtaining personal data about existing donors and supporters from third parties (telematching or teleappending)	CSOs can obtain data, such as up to date phone numbers on existing donors and supporters, provided that they inform the individual that the CSO has obtained their data and from which source at the earliest opportunity, and not later than the first communication with the individual. CSOs will also need to inform the individual of their right to withdraw consent for or object to direct marketing based on data obtained from a third party.
Collecting data about users of your website	CSOs which operate websites and which install cookies on visiting users' devices need to obtain individuals' consent for doing so. Under current law this can be obtained via an opt-out "cookie notice" that visitors to the website can view. However, the forthcoming ePrivacy Regulation will tighten the rules and require websites to obtain users' explicit consent to tracking cookies.

II. International, regional and domestic standards on data protection and privacy

A. International standards

As described above, the right to privacy is enshrined in numerous international human rights instruments, including the International Covenant on Civil and Political Rights ("ICCPR"). The enforcement body for the ICCPR, the UN Human Rights Committee, issued a General Comment in 1988 which explained that the right to privacy includes the protection of personal data.[16] Around the same time, the UN General Assembly issued Guidelines for the Regulation of Computerised Personal Data Files, the contents of which echo the OECD Guidelines mentioned above.[17]

Since that time, however, international human rights bodies such as the United Nations have been slow to produce further guidance or standards on data protection and privacy rights, particularly as they apply in the context of digital technologies. It was not until 2013 that the General Assembly adopted another resolution related to privacy and data protection.[18] The UN Human Rights Council appointed the first UN Special Rapporteur on the right to privacy in 2015. Further standards-setting initiatives have yet to emerge from these or any other international bodies.

Absent such initiatives, **some UN agencies have taken it upon themselves to develop data protection standards applicable to their own work**. For example, in 2015 the UN High Commissioner for Refugees adopted its first Policy on the Protection of Personal Data of Persons of Concern, and in 2016 the World Food Programme adopted Principles and operational standards for the protection of beneficiaries' personal data in WFP's programming. Despite calls for a UN agency specifically dedicated to data protection,[19] further action has not taken place in this regard.

[16] UNHRC General Comment No. 16, 8 April 1988, para. 10.

[17] Resolution 45/95, 14 December 1990.

[18] A/RES/68/167, 18 December 2013.

[19] Graeme Weardon, "UN needs agency for data protection, European commissioner tells Davos," *The Guardian,* 22 January 2015, available at https://www.theguardian.com/technology/2015/jan/22/un-agency-data-protection-davos-edward-snowden.

B. European standards

i The GDPR

As outlined above, **Europe has been at the forefront of developing data protection and privacy standards for more than thirty years**. The Council of Europe's Convention 108, adopted in 1981 and modernised in 2016, remains the world's only international legally binding treaty in the field of data protection, with fifty signatories, including non-European ones. At the EU level, when the GDPR comes into effect in May 2018, and when coupled with the forthcoming ePrivacy regulation, the EU will have the strongest data protection and privacy framework in the world.

With few exceptions, European Union data protection and privacy standards will apply to all entities – including CSOs – that process the personal data of EU residents. **CSOs that aren't based in EU countries but which process EU residents' data, or CSOs that are based in EU countries but the activities of which are directed internationally, are likely to still be subject to EU data protection law.** The GDPR does not excuse CSOs from compliance simply because of their charitable purpose or the nature of their work. Although CSOs smaller than 250 people will not be required to comply with some elements of the GDPR,[20] on the whole CSOs processing European Union data will be subject to the Regulation from May 2018 on. Furthermore, CSOs which work through or use volunteers are not exempt from the GDPR; volunteers must be aware of and comply with data protection obligations on an equal basis to staff.

CSOs should obtain expert advice about the full range of ways in which the GDPR impacts upon their activities. Below we provide a general analysis of some of the specific requirements of the GDPR that will impact in particular on CSOs' fundraising activities, and explain what actions CSOs will need to take in order to comply. The major change for most CSOs will be the requirement to improve processes for obtaining individuals' consent to data processing, and in particular to direct marketing by email, SMS or automated telephone calls, which must only be conducted where consent is given. The GDPR considerably strengthens the requirement for consent, requiring it to be an unambiguous positive action. This means that pre-ticked boxes or opt-out protocols will no longer comply with EU data protection law. CSOs will need to find a way to enable individuals to give meaningful and explicit

[20] See, for example, Art. 30, which exempts organisations smaller than 250 people from maintaining a record of processing activities unless certain conditions exist.

consent to all data processing operations, including not only direct marketing but sharing data with third parties, wealth-screening and other donor research.

What the GDPR requires of CSOs

GDPR REQUIREMENT	ACTIONS REQUIRED OF CSOS
You must have a lawful basis for collecting and using an individuals' personal data.	The two forms of lawful basis most likely to be applicable to CSOs are consent [Art. 6(1)(a)] and legitimate interests [Art. 6(1)(f)]. The GDPR strengthens the consent requirements that existed under the Data Protection Directive. If you rely on consent, the request for consent must be clearly distinguishable, in an intelligible and easily accessible form, using clear and plain language [Art. 7]. Consent should be a freely given, specific, informed and unambiguous indication of the individual's agreement to processing of their personal data. Silence, pre-ticked boxes or inactivity will not constitute consent [Rec. 32]. Consent should cover all processing activities carried out for all purposes. You may only rely on "legitimate interests" as a lawful basis where those interests are not overridden by the interests or fundamental rights of the individual, particularly if that individual is a child [Art. 6(1)(f)]. Examples of legitimate interests include direct marketing purposes, preventing fraud [Recital 47], internal administrative purposes [Recital 48], processing for ensuring information security [Recital 49], and reporting possible criminal acts to a competent authority [Recital 50]. It would not be appropriate to rely on legitimate interests where the individual does not reasonably expect processing to take place in the particular manner [Recital 47]; this would almost certainly mean that activities such as wealth-screening may not be fairly conducted solely on the basis of legitimate interests. Direct marketing may be carried out for a legitimate interest, but is subject to restrictions (see below).
You must appoint a data protection officer in certain circumstances.	CSOs which are processing on a large scale special categories of personal data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data or health data), or which process data in a manner that requires regular and systematic monitoring of individuals, must appoint a DPO [Art 37(1)].
When conducting direct marketing, in almost all circumstances you must have the individual's consent.	Although the GDPR stipulates that CSOs can send direct marketing to individuals using legitimate interests as a lawful basis, the current ePrivacy Directive requires (implied or opt-out) consent when sending direct marketing by email, SMS or automated telephone calls. The forthcoming ePrivacy Regulation will require explicit or opt-in consent. You do not need consent to send direct marketing by post or to make live (person to person) phone calls, provided you can establish this is within your organisation's

	legitimate interests; direct marketing is automatically a legitimate interest, and thus a lawful basis for processing data.
You must be more transparent with individuals about how you process their data.	The GDPR sets a higher bar for the disclosure of information to data subjects. At the time of collecting personal data from individuals, you must give them information (through, for example, your privacy notice) about • the purposes for which you're acquiring the data, • who you will share it with, • what legitimate interests you are pursuing (if applicable), • whether you intend to transfer the data to a third country, • how long the data will be stored for, • what rights the individual has to request access to, erasure or rectification of, or portability of their data, • the individual's right to withdraw consent, and • the existence of any automated decision-making and the logic involved [Art. 13]. This means, for example, if a CSO is using donor information for wealth-screening, or intends on sharing donor information with another CSO, it must explicitly inform the individual of that fact. Such information must be provided in a concise, transparent, intelligence and easily accessible form, using clear and plain language [Art. 12(1)]. If CSOs obtain personal data from a source other than the individual (for example if it is purchased from a third party) they must give all of the above information to the individual within a reasonable period [Art. 14].
Even when you acquire personal data from the public domain, you have data protection obligations with respect to it.	CSOs must inform individuals, as soon as reasonably possible, if you acquire their personal data from publicly available sources, and inform them as to which source the data originated [Art. 14(2)]. CSOs must afford such data the same level of protections as personal data acquired directly from the individual themselves.
You must keep a record of the processing activities under your responsibility.	This applies to CSOs of larger than 250 employees or CSOs which carry out processing likely to result to a risk to the rights and freedoms of individuals. This is not a very high bar; the GDPR uses the threshold "high risk" in other provisions, and by omitting the qualifier "high" in this provision it suggests that any CSO processing data that might have particular privacy implications (for example collecting personal data on particularly vulnerable communities) or doing particularly large-scale data processing should keep a record of processing activities. This also applies to entities which process special categories of data like health or political data [Art. 30]. This obligation applies to CSOs both in the EU, and outside of the EU, where CSOs outside of the EU process EU residents' data in the context of offering them goods or services or monitoring their behaviour [Art. 3].
If you are processing data in a manner that is likely to create a high risk to individuals, including by using new technologies, you must undertake a Data	DPIAs will be particularly required whenever CSOs are undertaking "systematic and extensive evaluation of personal aspects" of individuals based on automatic processing or profiling, where such decisions produce legal effects, or where CSOs process on a large scale special categories of data [Art. 35]. Because special categories of data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade

Protection Impact Assessment.	union membership, as well as genetic data, biometric data or health data, many CSOs may be caught by this provision and have to undertake a DPIA.
You must implement appropriate technical and organisational measures to protect individuals' data.	CSOs will need to consider "data protection by design and by default", embedding the protection of personal data into the heart of their data processing activities. That means thinking about minimising the amount of data is collected and deleting data that is no longer necessary (that is, you don't need it anymore – for example out of data contact details or old website analytics data) and implementing measures like pseudonymisation[21] to minimise the risk of data abuse, theft or loss [Art. 25]. CSOs should not collect any more personal data than is strictly necessary for their purposes. CSOs will also need to make sure their technical systems are sufficiently rigorous taking into account the nature of the personal data they process [Art/ 32].
If you share data with a third party, you must make sure they provide an equivalent level of protection.	CSOs which are data controllers for the purpose of the GDPR cannot use third parties to process that data (for example, for research, wealth-screening or marketing communications, or outsourcing employee payroll) unless those third parties provide sufficient guarantees that they will provide equivalent protection as required by the GDPR [Art. 28]. A CSO can ensure it has sufficient guarantees through introducing provisions in the contract with the processor containing certain provisions[22] or only contracting with entities certified as complying with a code of conduct.
You must give individuals a right to object to the processing of their personal data, especially when you are using their personal data for direct marketing.	The GDPR establishes that individuals shall have the right to object to the processing of their personal data at any time when the basis for the processing is your legitimate interests [Art. 21]. You must inform them of that right in a clear and distinct manner [Art. 21(40]. Unless you can demonstrate compelling legitimate grounds for the processing which override the individuals' rights and interests, you must cease processing. If the type of processing to which the individual objects is direct marketing, the individual has the right to object to any time and processing must cease immediately [Art. 21(2)&(3)]. CSOs should maintain a list of all individuals who have objected to direct marketing to make sure they are not further marketed to.
You must give individuals a right to request access to their personal data.	CSOs will need to put processes in place to ensure they can respond to individuals' request for their personal data, and may not charge for providing such data [Art.15]. Individuals have a new right under the GDPR to receive their personal data in a structured, commonly used and machine-readable format [Art. 20].

[21] Pseudonymisation is "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." [Art. 4] To pseudonymize a data set, the "additional information" must be "kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person." In sum, it is a privacy-enhancing technique where directly identifying data is held separately and securely from processed data to ensure non-attribution.

[22] The UK Information Commissioner's Office has published guidance on contracts and liability between controllers and processors: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

You must be able to erase individuals' personal data upon their request in certain circumstances.	Individuals have a new right under the GDPR to request the erasure of their personal data without undue delay where those data are no longer necessary in relation to the purposes for which they were collected, where they withdraw consent, or where they object to the processing, among other grounds [Art. 17].
You must report any breach of personal data to the data protection authority in most circumstances.	If a CSO experiences a breach of personal data (either because of data loss, theft, misuse, or deletion), it will need to report that breach to the relevant data protection authority, unless it is unlikely to result in a risk to the rights of individuals.

ii The European Union Charter of Fundamental Rights and the Court of Justice of the European Union

Although the EU Charter mostly replicates the rights in the European Convention on Human Rights ("ECHR"), **in the context of privacy and data protection it actually expands the ECHR rights**. That is, in addition to Article 7 protecting the right to respect for privacy and family life, home and communications (a replication of Art. 8 ECHR), the Charter contains Article 8 – Protection of personal data. Article 8 stipulates:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

It is clear that Article 8 enshrines the principles which underpin the GDPR, and other European Union data protection regulations.

Individuals or organisations do not have any particular right to recourse under the European Charter per se, but rather are able to challenge the validity of domestic law and EU regulation on the basis of non-compliance with, inter alia, the Charter, by pursuing a reference from a domestic court to the Court of Justice of the European Union ("CJEU"). The CJEU has issued numerous important decisions on issues related to privacy and data protection, including decisions establishing that States cannot require

communications providers to retain personal data indiscriminately,[23] and that companies cannot transfer personal data outside of the EU to the US because of the absence of sufficient safeguards in the US against unlawful surveillance, in the absence of other arrangements.[24]

The CJEU also decided the seminal case on the right, under data protection law, to have data erased, also known as "the right to be forgotten." In the case, the Court found that the EU Data Protection Directive applied to search engine operators, and that the Directive established the right under certain conditions for individuals to ask for search engines to remove links with their personal data where such data was inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing.[25] That right is now explicitly included in the GDPR, which requires organisations to erase their personal data without undue delay where the data are no longer necessary in relation to the purposes for which they were collected or processed, where the data subject withdraws consent, or under other discreet circumstances [Art. 17(1)]. The GDPR carves out a number of exceptions to the right, including where the processing is necessary for exercising the right of freedom of expression or information, for reasons of public interest in the area of public health or for archiving purposes [Art. 17(2)].

iii The European Convention on Human Rights and the European Court of Human Rights

The European Court of Human Rights has developed a rich body of jurisprudence concerning the rights to privacy and protection of personal data protected in Article 8 of the European Convention on Human Rights, much of which has centred on State surveillance of individuals' communications.[26]

The Court is currently considering a seminal case on State surveillance of the communications of civil society organisations. In 10 Human Rights Organisations v The United Kingdom, heard in Strasbourg in late 2017, the European Court of Human Rights is assessing the impact of "mass" or "bulk" surveillance regimes on the rights to privacy and freedom of expression of both British and

[23] *Digital Rights Ireland v Irelands & Ors* Court of Justice of the European Union, 8 April 2014; Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, 21 December 2016

[24] *Schrems v Data Protection Commissioner, Ireland,* Court of Justice of the European Union, Case C-362/14, judgment of 6 October 2015.

[25] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, 13 May 2013

[26] See, for example, *Rotaru v Romania,* European Court of Human Rights, App. no. 28341/95; *Malone v Untitled Kingdom,* European Court of Human Rights, 2 August 1984; *Weber and Saravia v Germany,* European Court of Human Rights; App. no. 54934/00.

foreign human rights organisations, including Liberty, Privacy International, and Amnesty International. The Court will also consider the ramifications of foreign intelligence sharing on the privacy rights of the CSOs. The Court's decision is expected in 2018.

For the purpose of understanding the interplay between data protection and privacy standards and the right of CSOs to fundraise, it is worthwhile briefly highlighting the Court's jurisprudence regarding the balance between the right to privacy, on the one hand, and the right to freedom of expression, on the other. The European Court has on more than one occasion found that CSOs have contravened an individual's right to reputation, which forms part of the Article 8 protection of the right to privacy, through public[27] or private[28] defamatory statements. Although such statements are rarely related to fundraising, they may be part of the CSOs broader campaigning or lobbying activities (which in turn relates to their public visibility and ability to raise funds). Although the Court tends to judge each specific case on its merits and considers a range of factors when contemplating how to balance the competing rights, public statements by CSOs must be made in good faith and based on accurate facts in order to be afforded the protection of the law.[29]

iv The Cybercrime Convention

The Council of Europe Convention on Cybercrime (also known as the Budapest Convention), was adopted in 2001, and is designed to achieve the harmonisation across states parties of laws which criminalise, among other things, unauthorised access to computer data and systems. Almost all Council of Europe member states have signed or ratified the Convention, along with more than a dozen non-members, including the United States. The Convention requires States to criminalise unauthorised access to a computer system, illegal interception of communications and data interference, as well as misuse of devices. The Convention also contains a range of offense relating to illegal content, such as child sexual exploitation material.

---

[27] Růžový Panter, OS v. Czech Republic, ECHR, 2 February 2012, Application No 20240/08.

[28] Medžlis Islamske Zajednice Brčko and Others v. Bosnia and Herzegovina (application no. 17224/11).

[29] This is a complex and vast area of law; CSOs wishing to learn more about the interplay between the rights to privacy and freedom of expression should consult, inter alia *Friend or Foe? Protecting freedom of expression and privacy in the digital age,* ARTICLE 19, May 2016, available at https://www.article19.org/resources.php/resource/38658/en/article-19-launches-global-principles-on-freedom-of-expression-and-privacy.

The Cybercrime Convention was criticised on its adoption for its broadly drawn language and lack of specific protections for freedom of expression in the context of the content provisions.[30] Beyond this, it does not contain provisions that bite on CSOs' data protection obligations specifically, nor does it relate to the right to fundraise.

C. Other regional standards

i The African Union Convention on Cybersecurity and Personal Data Protection

In July 2014 the AU adopted a Convention on Cybersecurity and Personal Data Protection, which will come into force after fifteen States ratify the treaty; only Senegal has taken steps to ratify the treaty to date,[31] while eight countries have signed but not ratified it.[32] Moreover, the process of adopting the Convention was plagued with accountability and transparency shortfalls. As a result, the Convention has not yet proven to be an effective means of influencing activities in the field of data protection on the continent.

The Convention requires data controllers to declare their data processing activities before a data protection authority [Art 10]. "Non-profit making association[s]" or bodies, with "a religious, philosophical, political or trade union aim" are exempted from making such a declaration, provided the data are "consistent with the objective of the said association or body structure, and relate solely to its members, and that the data are not disclosed to a third party". This provision may exempt some CSOs from having to declare data processing to the data protection authority.

Beyond this exemption, the Convention enshrines the same broad principles and rights found in the GDPR, although with far less detailed instruction to data controllers. Interestingly, the wording of the Convention implies a stronger reliance on consent than the GDPR. Article 13 stipulates that data processing shall only be legitimate where an individual has given their consent, but that this

[30] See for example, Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cybercrime Version 24.2, 12 December 2000, available at http://gilc.org/privacy/coe-letter-1200.html

[31] "A decisive step by Senegal towards accession to and ratification of the Budapest and Malabo Conventions," *Observatoire-FIC.com*, 2 May 2016, available at https://www.observatoire-fic.com/a-decisive-step-by-senegal-towards-accession-to-and-ratification-of-the-budapest-and-malabo-conventions/.

[32] Skye Terebey, "African Union Cybersecurity Profile: Seeking a Common Continental Policy," *Henry Jackson School of International Studies, University of Washington*, 22 September 2016, available at https://jsis.washington.edu/news/african-union-cybersecurity-profile-seeking-common-continental-policy/.

fundamental requirement may be waived where processing is necessary for, inter alia, the performance of a legal obligation. The concept of legitimate interests is not to be found in the Convention, meaning that CSOs could not rely on it for direct marketing and would instead be required to obtain consent.

ii The APEC Privacy Framework and Cross-Border Privacy Rules

The APEC Privacy Framework was adopted by 21 participating countries in 2004, and was designed to provide a baseline understanding of privacy protections to ensure that personal data could flow to and within Asian countries. Essentially, the Framework set down very high-level principles (similar to the OECD principles) regarding data protection in a region in which domestic data protection laws were either non-existent or nascent. There is no rigorous enforcement mechanism for the Framework, but rather it encourages individual States to prepare Individual Action Plans for reporting on compliance and implementation. The privacy principles enshrined in the Framework mirror, to some extent, those in the GDPR, but are not as demanding; for example, the Framework does not require notification of data breaches to data protection authorities. [33]

The Framework set in motion the process of creating the APEC Cross-Border Privacy Rules ("CBPR") system, which institutionalises some of the requirements of the European Data Protection Directive in order to enable participating companies to transfer data out of the EU and ensure adequate protection for that data. A self-regulatory scheme, the CBPR system works by enabling participating companies to voluntarily submit to assessment by a third-party company that has been recognised as a CBPR "Accountability Agent". The Accountability Agent undertakes the assessment of the participating companies, verifies them as compliant and oversees ongoing compliance, reporting to the member state privacy enforcement authorities any incidents of non-compliance.

Five APEC countries are participating in the scheme: US, Mexico, Japan, Canada and South Korea. Only two Accountability Agents have been certified: the Japanese JIPDEC and US company TRUSTe. Numerous big-name US companies have voluntarily submitted to ABPR certification, including Apple, IBM and Hewlett Packard. There does not seem to be any clear prohibition against CSOs participating in the scheme, but there are no CSOs currently doing so. In any event, the scheme has been subject to

[33] Alex Wall, "GDPR matchup: The APEC Privacy Framework and Cross-Border Privacy Rules," *IAPP,* available at https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/#

sustained criticism,[34] and has significant flaws; the US Federal Trade Commission has repeatedly gone after non-certified companies for falsely claiming they are certified, for example.[35]

D. Domestic rules

In most countries, data protection and privacy rights and obligations will not only be confined to a single piece of legislation, but rather peppered throughout numerous different legal frameworks. CSOs should look to the following areas of law and regulation to understand what their rights and responsibilities are when it comes to privacy and data protection:

i. Constitutional law and jurisprudence

More than 150 national constitutions mention the right to privacy,[36] and many of those directly incorporate or apply verbatim the language of the International Covenant on Civil and Political Rights. In addition, national courts have read a right to privacy into constitutional protections in a number of circumstances. For example, the Indian Supreme Court recently found that the right to privacy is inherently protected by the provisions of the Indian Constitution which protect the rights to life and liberty.[37] Although explicit mention of privacy cannot be found in the US Constitution, the right underpins the prohibition against unreasonable searches and seizures found in the Fourth Amendment,[38] and has been read into the First Amendment's protection of speech[39] and the Fourteenth Amendment's liberty clause.[40]

ii. Sectoral privacy laws and common law

While many countries have comprehensive data protection laws (which cover all private and public sector entities), others have sectoral laws pertaining to specific issues or sectors. For example, the

---

[34] For example, Graham Greenleaf, "APEC's Cross-border privacy rules system: A house of cards?" (2014) 128 *Privacy Laws & Business International Report*, 27-30

[35] Three Companies Settle FTC Charges that They Deceived Consumers About Participation in International Privacy Program, Federal Trade Commission, 22 February 2017, available at https://www.ftc.gov/news-events/press-releases/2017/02/three-companies-settle-ftc-charges-they-deceived-consumers-about

[36] Constitute Project, available at https://www.constituteproject.org/search?lang=en&key=privacy&status=in_force.

[37] Ravi Agrawal, "India Supreme Court rules privacy a "fundamental right" in landmark case," *CNN,* 25 August 2017, available at http://edition.cnn.com/2017/08/24/asia/indian-court-right-to-privacy/index.html.

[38] Katz v United States 389 U.S. 347

[39] Stanley v Georgia 394 U.S. 557

[40] Lawrence v Texas 539 U.S. 558

United States has federal legislation specifically pertaining to children's privacy online, called the Children's Online Privacy Protection Act, and to health information, the Health Insurance Portability and Accountability Act of 1996. In Canada, there are 28 federal, provincial and territorial privacy statutes, in addition to legislation such as anti-spamming laws or identity theft provisions in criminal codes which pertain to privacy protections. Most countries will have some form of financial privacy or banking secrecy law which requires confidentiality of personal data by financial entities.

Common law also has a role to play in governing privacy and data protection. For example, civil actions of unfair and deceptive practices touch upon how companies use and process personal data, and the tort of defamation relates to the use of personal data in the public realm.

iii. Cybercrime and national security laws

Every country will impose restrictions on the enjoyment of privacy and data protection in certain circumstances related to policing, the protection of national security, and the prevention of cybercrime. Such laws generally empower security agencies to intercept communications, conduct covert surveillance and otherwise monitor individuals and organisations in pursuit of specific legitimate aims. Cybercrime laws prevent unlawful access to personal data through, for example, hacking, and also create offences relating to the conduct of illegal activity online.

iv. Fundraising laws and laws on CSOs

Restrictions on and requirements for fundraising may include data protection obligations or may be limited by data protection requirements. Fundraising may be regulated in laws on CSOs, laws regulating charity and charitable organisations, money collection laws and regulations, and other acts such as presidential decrees.[41] Often fundraising regulation is part of laws specifically regulating the establishment, registration, and governance of CSOs; this is the case, for example, in the United Kingdom.[42] Generally speaking, data protection laws can be attenuated by legal obligations imposed by other legal frameworks, including fundraising laws. For example, both the Data Protection Directive and the General Data Protection Regulation leave room for EU Member States to impose legal obligations on entities (including CSOs) to require the processing of personal data for any reason,

[41] European Center for Not-for-Profit Law, The Regulatory Framework for Fundraising in Europe, 2017.

[42] Charities Act 2011

including, for example, for fraud prevention, crime detection or the regulation of fundraising. Data processing obligations imposed by domestic legislation will be legitimate under data protection law because they will comprise a "legal obligation" under which a CSO is required to process data.

E. Self-Regulatory Initiatives

A number of self-regulatory initiatives in the field of CSOs and fundraising are to be found at different levels and often include obligations relevant to data protection and privacy.

At the international level, the Association of Fundraising Professionals maintains the International Statement of Ethical Principles in Fundraising, which was adopted at the 2006 International Fundraising Summit, and revised in April 2017. The Principles include the following, which are relevant to privacy and data protection:

- Fundraisers will respect donor rights by providing timely information about how contributions are used, respecting donor privacy and honouring donor wishes;
- Fundraisers will respect beneficiary rights and preserve their dignity and self-respect;
- Fundraisers will only use information that is accurate, truthful and not misleading;
- Fundraisers will respect data protection rules and laws at all times.[43]

At the regional level, regional associations such as the European Fundraising Association and the Southern African Institute of Fundraising ("SAIF") are members of the Association and subscribe to the International Statement of Ethical Principles. Beyond that, we are not aware of any other significant regional initiatives in this field.

There are also self-regulatory initiatives at the domestic level. Some of these initiatives are undergoing review and revision in light of the changing nature of fundraising and the emerging challenges in the digital age. One of the most prominent and dramatic of such changes may be the proposed revisions to the UK Fundraising Regulator's Code of Fundraising Practice, which were subject to a public consultation between October and December 2017. The wide-ranging changes are specifically designed to update the Code to take account of the GDPR, as well as other issues identified by the data protection authority in the UK, i.e. the Information Commissioner's Office. The changes

[43] AFP International Statement of Ethical Principles in Fundraising, Revised April 2017, available at http://www.afpnet.org/Ethics/IntlArticleDetail.cfm?ItemNumber=3681

reorder the Code to bring data protection into a single place and provide detailed guidance on governance, storage and maintenance of data, buying and sharing personal data, and direct marketing (including consent as the lawful basis for direct marketing).

British CSOs are also able to draw from guidance issued by the industry body, the Institute of Fundraising, about compliance with the GDPR; *GDPR: The Essentials for Fundraising Organisations* is a notable instance of a valuable industry tool to assist CSOs in complying with data protection standards.[44]

The revised UK Code (assuming it is adopted in its draft form, or something close thereto) enshrines stricter standards than other national codes in countries in which the GDPR will not come into effect. For example, the Fundraising Institute of Australia has just revised its Code in July 2017. The Code does not contain any obligation to proactively disclose information to donors about how data is obtained or used, but rather requires fundraisers to respond to requests for information, where asked. The Code does not seem to mirror exactly the Australian Privacy Act 1988, which requires that information about how data is obtained must be included in a privacy policy. Reflecting Australian data protection law, fundraisers are not required under the Code to obtain the prior consent of individuals before selling or sharing their personal data or using it for marketing purposes. Although the Privacy Act does include some restrictions on how personal data should be used by entities in the context of direct marketing,[45] these restrictions are not reflected in the Code.

The Swiss Fundraising Organisation maintains a set of ethical principles which, although they do not appear to have been updated since August 2010, contain a relatively strong pronouncement regarding data protection (translated from the French): "*Fundraisers must comply with applicable data protection regulations and laws. They respect the fact that the fundraising data and the data of donors belong to the public utility of the organization collecting the funds. These data may not be sold, rented, exchanged, copied or marked*."[46]

---

[44] Institute of Fundraising, "Institute of Fundraising Launches New GDPR Guide and Training for Charities," 4 May 2017, available at https://www.institute-of-fundraising.org.uk/about-us/news/institute-of-fundraising-launches-new-gdpr-guide-and-training/

[45] See section 7, Schedule 1 – Australian Privacy Principles

[46] Swiss Fundraising, *Principes éthiques pour le fundraising,* available at https://swissfundraising.org/fr/membres-2/principes-ethiques/

The Fundraising Institute of New Zealand, despite maintaining a Code of Ethics and Professional Conduct, a Code of Fundraisers' Relationships with Donors, and twelve different standards pertaining to issues such as overseas aid and direct mail, does not address data protection and privacy in any substantive way at all.

F. Conflicting standards: anti-money laundering and counter terrorist financing obligations

In recent years, CSOs have come under increasing pressure to ensure that charity fundraising does not become a vehicle for money laundering or terrorist financing. This pressure has translated into legal obligations to document donations, retain information and report suspicious information, all of which raise potential conflicts with data protection standards.

Obligations regarding anti-money laundering and counter terrorist financing have their origins in a number of international instruments:

- UN Security Council Resolution 137 and the Convention for the Suppression of the Financing of Terrorism, which imposed on State obligations to prevent and suppress the financing of terrorist acts and to criminalise terrorism-related activities;
- The Convention Against Transnational Organized Crime and the Convention against Corruption, which, inter alia, require regulation in the area of financial institutions and money laundering;
- The Financial Action Task Force on Money-Laundering ("FATF") Recommendations, which are a set of 40 recommendations and 9 special recommendations designed to provide a comprehensive set of measures for a legal and institutional regime against money laundering and the financing of terrorism.

States have implemented their obligations under the above-named instruments into domestic law in varied and often piecemeal ways. EU countries will have broadly similar regulation in the field of money-laundering as the EU has adopted a series of successive money-laundering Directives; the Fourth Money Laundering Directive came into effect in June 2017. However, beyond this, regulation is likely to differ country by country.

CSOs are often the target of such regulation. FATF Recommendation 8 noted the vulnerability of non-profit organisations to being used for terrorist financing purposes, and strongly encouraged States to introduce government registration processes for CSOs, introduce financial reporting and exchange

data with law enforcement organisations. The accompanying FATF evaluation system has "endorsed some of the most restrictive non-profit organisation regulatory regimes in the world," according to a 2012 Statewatch report, and "strongly encouraged some already repressive governments to introduce new rules likely to restrict the political space in which NGOs and civil society actors operate."[47] By way of illustration, two of only five countries judged compliant with FATF R8 as of 2012 were Egypt and Tunisia. In a separate ECNL[48] and Statewatch report, researchers observed concerning impacts of R8 in countries such as Bosnia and Herzegovina, Croatia, Hungary, India, Poland, Serbia and Tajikistan.[49]

With respect to potential conflicts with data protection standards, this too differs dramatically country by country. Speaking generally, potential areas in which conflicts may arise include:

- CSOs might be required to retain personal data on donors for longer than would be necessary for the purposes for which they were being processed;
- CSOs might be required to report suspicious behaviour to national authorities and disclose donors' personal information;
- CSOs might be required to refrain from informing donors about reports raised about them or investigation into them, even when presented with a request by a data subject for access to their personal data. For example, in the UK charities are under various obligations to report "suspicious activity" related to potential money laundering or terrorist activities to the relevant authorities. The Terrorism Act and the Proceeds of Crime Act both contain provisions which make it an offense to notify a person that a "suspicious activity report" has been made to the authorities about them, if that disclosure might prejudice any investigation.[50]

[47] Ben Hayes, Counter-Terrorism, 'Policy Laundering' and the FATF: Legalising Surveillance, Regulating Civil Society, Statewatch, 2012.

[48] http://fatfplatform.org/wp-content/uploads/2015/10/Catalogue-of-government-overregulation-July-2015_final-.pdf

[49] Countering terrorism or constraining civil society? The impact of Financial Action Task Force recommendations on non-profit organisations in Central and Eastern Europe and Central Asia, Statewatch, 2014.

[50] Law Society of England and Wales, *Anti-Money Laundering: Guidance for the Legal Sector,* September 2017, available at http://www.lawsociety.org.uk/policy-campaigns/articles/draft-anti-money-laundering-guidance/

III. Conclusions and Recommendations

A. Reconciling the right to fundraise with data protection obligations

Data protection standards are there to protect CSOs just as they protect individuals from the risks of unauthorised access to or use of data, the risk of unlawful State surveillance, the reputational risks that might flow from data breaches, and the risk to sustainability if donors and supporters lose trust in CSOs.

However, it is inevitable that data protection and privacy standards must influence how CSOs fundraise, and indeed may curtail to some degree CSOs' fundraising activities. **Although data protection regulation will rarely prevent CSOs from undertaking a particular fundraising activity, it will often require them to obtain an individual's consent to do such an activity, effectively stemming certain practices**. This is the case, for example, with wealth screening; undoubtedly, data protection regulation requires CSOs to obtain explicit consent for such a practice, which, after all, involves an invasive analysis of an individual's private life. Many potential and current donors will likely not consent to being subject to wealth screening.

Data protection regulation may also create onerous compliance obligations that may be difficult for smaller CSOs to meet: establishing a procedure for subject access requests, for example, or giving effect to erasure obligations may be difficult for small, under-resourced organisations. At the same time, such organisations are likely to be less capable to cope with a data breach and may suffer harshly from the reputational risks that poor data management entails. Small CSOs may have more to lose through non-compliance with data protection standards than by dedicating scant resources to up-front compliance.

Many CSOs believe that there should be exemptions from data protection standards for charitable enterprises, and this argument is persuasive in certain circumstances: fundraising is critical to the business model of charities and the high costs of compliance might result in vital charitable endeavours being abandoned. On the other hand, it could be argued that CSOs bear an even higher responsibility than other entities to respect data protection standards, as they often deal with the personal data of society's most vulnerable people.

As data protection standards become globally standardised and continually strengthened, this debate will arguably become moot. Data protection, and particularly the EU-style of data protection enshrined in the GDPR, is here to stay, and will only become more entrenched in domestic legal systems. CSOs will have no choice but to comply. The challenge, then, is for CSOs to adopt new fundraising approaches and internal governance procedures that ensure compliance with data protection standards. This challenge will be made more achievable if CSOs are able to change the mind-sets of staff and volunteers by promoting data protection and privacy as important pillars of charitable endeavours.

B. Recommendations to civil society organisations

- **Start now.** Whether you will be subject to the GDPR or not, improving your level of data protection within your organisation will minimise risks and begin to engender a culture of data protection and privacy. Data protection laws continue to be adopted every year in countries around the world, and we are gradually seeing data protection coalesce around similar standards, led by the EU. Even if you don't work in a country with strict data protection laws now, it is highly likely you will in future.
- **Aim for the highest common denominator.** By aiming for the standard set by the GDPR, even if you are not an EU-based CSO, you can ensure you will always comply with all domestic regulation globally. This is particularly vital for international CSOs.
- **If you will be subject to the GDPR, get legal advice as soon as possible** to ensure that you are doing everything you can to be compliant once the Regulation comes into effect in May 2018. But also, remember that the GDPR is an "evolution, not a revolution". Compliance will be a process of trial and error for all entities, and you will need to continually adapt as new lessons and standards emerge from data protection regulators over time. Ensure that you have an internal mechanism (such as a point person) whose responsibility it is to stay up to date with these developments.

- **Consult available resources**. Some useful English-language resources for CSOs on compliance with the GDPR include
    - The UK Fundraising Regulator's Personal Information and Fundraising: Consent, Purpose and Transparency;[51]
    - The Institute of Fundraising's GDPR: The Essentials for Fundraising Organisations;[52]
    - The Data Protection Network's Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation;[53] and
    - Tim Turner's Fundraising and Data Protection: A survival guide for the uninitiated.[54]

C. Recommendations to governments and data protection regulators

- To the greatest degree possible, ensure CSOs have certainty about their data protection obligations. This can be achieved through issuing guidance, commissioning independent reports, holding training sessions or providing free advice to CSOs.
- Ensure that domestic legislation, including laws regulating fundraising and charities, laws on data protection, and laws on cybercrime and national security, are consistent with and reflect international human rights law, in particular the rights of organisations to associate, assemble and fundraise.
- Develop best practice examples and templates for CSOs to use in order to minimise the cost of compliance.
- Consider what additional enforcement process could be introduced specifically for CSOs to ensure that non-compliant organisations are not faced with punitive measures but rather assisted to move towards compliance with the assistance of the government or regulator.
- Support self-regulatory initiatives to assist CSOs in moving towards compliance while supporting them to do so in a manner consistent with the right to fundraise.

---

[51] Available at https://www.fundraisingregulator.org.uk/information-registration-for-fundraisers/guidance/personal-information-fundraising-consent-purpose-transparency/

[52] Available at https://www.institute-of-fundraising.org.uk/about-us/news/institute-of-fundraising-launches-new-gdpr-guide-and-training/

[53] Available at https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/

[54] Available at https://www.civilsociety.co.uk/news/free-guide-to-gdpr-and-data-protection-for-charities-published-today.html.