VINCENT PFAMMATTER
ADRIEN ALBERINI
KEVIN GUILLET

DATA PROTECTION AND THE SWISS NON-PROFIT SECTOR

How the GDPR considers the specificities of charities and international organizations

The new General Data Protection Regulation marked an unprecedented change in the EU data protection landscape. Charities are concerned by these changes, even if they are Swiss-based entities and do not aim for profits. Similarly, international organizations cannot fully ignore this new legislation. Exceptions and specificities apply however to such entities.

1. INTRODUCTION

There are many variations and definitions of charitable organizations, including non-profit organizations, grant-making or operating organizations and non-governmental organizations (NGOs). For purposes of the present article, we will use the overarching definition of *"charity"*, which shall include of all these variations.

In Switzerland, charities can be defined as private legal entities pursuing non-profit purposes. Swiss law foresees two main legal forms for such organizations, namely associations (Art. 60 et seq. of the Swiss Civil Code, CC) and foundations (Art. 80 et seq. CC).

The non-profit sector in Switzerland is also characterized by the presence of international organizations, which form an integral part thereof, even though such entities benefit from a widely different status under Swiss and international law.

This article addresses the extent to which the GDPR [1] considers the unique nature of Swiss-based charities and international organizations. It is composed of five parts. First, we will briefly lay out the principles of the GDPR (Section 2). Second, we will discuss its applicability to Swiss-based charities (Section 3). Third, we will dig into data protection specificities related to charities (Section 4). Fourth, we will address the (debated) application of the GDPR to international organizations (Section 5). Fifth, we will present some cases in which sanctions have been applied under the GDPR, as well as data protection related sanctions that were imposed on charities in Europe (Section 6). To conclude, we will recommend a few actions that may be taken by charities at this juncture.

2. EUROPEAN REGULATORY FRAMEWORK

The GDPR is the first significant update of data protection laws in Europe in over 23 years, as the previous EU directive applicable to this field was adopted in 1995, i. e. when the Internet was just beginning to be widespread and no smartphone was available; in addition, Google and Facebook had not been created at that time. Based on fundamental liberties [2], the GDPR embodies the right to informational self-determination and defines the right to privacy as a fundamental right [3].

The GDPR is an extensive piece of legislation with a wide scope of application. It encompasses 173 Recitals as well as 99 articles representing altogether about a hundred pages of regulation.

Under the GDPR, personal data is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fac-

VINCENT PFAMMATTER, LL.M. (UC BERKELEY), ATTORNEY-AT-LAW, PARTNER, SIGMA LEGAL, GENEVA, ACADEMIC FELLOW AT THE GENEVA CENTRE FOR PHILANTHROPY

ADRIEN ALBERINI, PH.D., LL.M. (STANFORD), ATTORNEY-AT-LAW, PARTNER, SIGMA LEGAL, GENEVA

tors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" [4]. It results from this definition that the concept of personal data is meant to be broad and comprise any piece of information which may possibly be linked to a specific person [5].

In a nutshell, the main principles of the GDPR may be summarized as follows:

1. The principle of lawful processing: personal data shall only be processed lawfully. The GDPR sets out the grounds of lawful processing, such as the consent of the data subject, the performance of a contract, compliance with a legal obligation, the protection of vital interests, the performance of a task carried out in the public interest or the legitimate interests of the entity processing the data [6].
2. Purpose specification and limitation: personal data shall be collected for "specified, explicit and legitimate purposes" [7]. It must be clear from the very beginning what are the purposes for processing [8].
3. Data minimization: personal data shall be processed in a way which is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [9]. This also includes the obligation to delete any personal data that is no longer needed [10].
4. Accuracy: personal data shall be "accurate and, where necessary, kept up to date" [11]. It is also required to take every reasonable step to rectify or erase inaccurate data [12].
5. Storage limitation: personal data shall be kept only for the time needed in a form which enables identification [13]. On the contrary, anonymized data may be kept indefinitely [14].
6. Integrity and confidentiality: personal data shall be processed "in a manner that ensures appropriate security" [15], using appropriate technical and organizational measures.
7. Accountability: the data controller must be able to demonstrate its compliance with the GDPR [16]. The data controller is legally responsible for any processing of personal data.

While the GDPR attracts most attention, one must bear in mind that the European regulatory framework applicable to data protection comprises, besides the GDPR, other rules and regulations, such as the Privacy and Electronic Communications Directive (the so-called ePrivacy Directive), which is also being revised [17].

In this context, it should further be mentioned that the Swiss Federal Data Protection Act of June 19, 1992 (DPA) [18], is currently being revised. The overhaul is being driven by the GDPR, as well as the latest amendments to the Council of Europe Treaty 108 [19]. The revised DPA – in its current state – will mostly take over the GDPR principles.

The revised DPA is set to go through the parliamentary process. The Political Institutions Committee of the National Council has postponed the consultation to the first quarter of 2019 during the spring session of the National Council [20].

KEVIN GUILLET,
ATTORNEY-AT-LAW,
PARTNER, SIGMA LEGAL,
GENEVA

3. APPLICATION OF THE GDPR TO SWISS-BASED CHARITIES

The GDPR states that the Regulation applies to the processing of personal data in the context of the activities of an establishment in the European Union (the so-called establishment criterion) [21]. Moreover, it also applies worldwide when the processing relates to goods and services offered to data subjects in the European Union [22] or when it implies the monitoring of their behavior in the European Union (the so-called targeting criterion) [23].

On November 16, 2018, the European Data Protection Board ("EDPB"), an independent European body that contributes to the consistent application of data protection rules [24], published its Guidelines 3/2018 regarding the "territorial scope of the GDPR" [25]. These guidelines are relevant for Swiss entities and provide guidance on the conditions under which the GDPR applies outside the European Union. The Swiss Federal Data Protection and Information Commissioner also published guidelines as to the application of the GDPR in Switzerland [26].

Regarding the establishment criterion, the EDPB recommends a broad definition: it extends to any "real and effective activity – even a minimal one – exercised through stable arrangements" [27]. The EDPB adds that the "threshold for 'stable arrangements' can actually be quite low [28] when the center of activities of a controller concerns the provision of services online [...] the presence of one single employee or agent of the non-EU entity may be sufficient [...]" [29]. Concerning Swiss-based charities, the GDPR may be applicable under the establishment criterion as soon as one employee would act in the European Union on its behalf.

With respect to the targeting criterion, it requires a targeting element, such as offering goods or services or monitoring the behavior of data subjects [30]:

→ The EDBP considers that "there needs to be a connection between the processing activity and the offering of good or service, but both direct and indirect connections are relevant and to be taken into account" [31]. Regarding in particular charities, one shall bear in mind that "[u]nder the GDPR, the fact that an organization may or may not require payment in exchange for its goods and services is irrelevant" [32].

→ Regarding the monitoring of data subjects' behavior, the EDBP considers that not all online activities should be deemed as monitoring activities. It is necessary to assess the controller's purpose for processing the data, as they should involve behavioral analysis or profiling techniques [33].

For Swiss-based charities, the GDPR may also be applicable under the targeting criterion, should the offering of goods or services take place in the European Union, or if the charity

monitors the data subjects' behavior on its website for example (e.g. with use of Google Analytics tools).

4. GDPR SPECIFICITIES RELATED TO CHARITIES

4.1 Preliminary note: Charities compared to for-profit entities. On the one hand, charities carry out activities which differ to a significant extent from companies looking for profits. This is particularly the case when they have to intervene in critical situations (Section 4.2 below) or perform charity-specific activities like fundraising (Section 4.3 below). From that perspective, the specific nature of the work performed by charities raises specific types of data protection issues.

On the other hand, charities are in many ways similar to for-profit companies. They deal with data concerning their employees, financial data, data from service providers (e.g. IT), etc. As such, charities encounter in their daily (business) life standard data protection issues, ranging from security and access to data, outsourcing of data management (for instance for human resources treatments), storing data over time, as well as sharing data with third-parties or in countries located outside of the EU (Section 4.4 below).

The duality described above raises the question whether charities should be subject to particular data protection rules. As we will see hereafter, the EU regulatory framework specifically recognizes some particular activities of charities. Thus, a few provisions in the GDPR are dedicated to these activities. That said and more generally, the GDPR applies regardless of the nature of the entity concerned or of its activities. Therefore, it is left to data protection authorities – when they issue guidance or enforce the GDPR – to determine whether charities should benefit from any particular treatment.

4.2 Processing of data relating to critical situations. Charities, and in particular NGOs, active in the humanitarian field constantly have to collect and process (sensitive) data of individuals in the context of crisis, war or natural disaster. The same is true with respect to charities working with vulnerable individuals that are in life danger in other contexts. In this regard, one should keep in mind that such situations may occur in or outside Europe.

Even if relying on consent [34] of the individuals whose personal data is collected and processed is the most prudent approach when managing personal data, there are instances, such as those described above, in which obtaining consent is not possible. In such cases, everything is more complicated, and it can be challenging to obtain and manage consent from employees, volunteers, and foremost from the beneficiaries (displaced people, refugees, injured individuals, victims of crimes and of war, etc.).

In this connection, many organizations active in the humanitarian field have understood early on the importance of data protection in critical contexts and have moved towards (auto)regulating and controlling their activities. In this respect, the ICRC is noteworthy. As a leader of humanitarian action, the ICRC has conducted a large study on the importance of protection data in the humanitarian environment and has published a "Handbook on Data Protection in Humanitarian Action" which may serve a guideline to all NGOs active in this field [35].

Interestingly, the GDPR expressly takes into account the specificity of these cases and recognizes that consent is not the only ground for lawfully processing data in such contexts; the protection of vital interests or, even more generally, public interest may serve as a valid basis underlying the processing of personal data. According to Recital 46 indeed, "the processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters" [36].

This Recital is in our view welcome and justified. While we may discuss it at length, the following two considerations deserve to be mentioned:

→ The humanitarian concept should not be interpreted too narrowly. Vital interest and public interest should in our view also justify the processing of personal data in relation to other critical situations which require the intervention of charities.

→ The fact that vital or public interests may justify certain processing does not mean that the charity carrying out the activity in question is out of the scope of the GDPR. First, other activities of these charities, such as those addressed in Section 4.4 below, should not benefit from the same types of justifications, i.e. consent may be required in relation to certain types of activities. Second, even in cases in which charities process data based on vital or public interests, it does not mean that the other obligations set out in the GDPR should not be observed. In particular, charities would have to comply with the general principles (such as transparency [37], meaning notably the need to adopt privacy policies) and mandatory safeguards, such as the implementation of technical and organizational measures [38].

4.3 Fundraising and marketing campaigns. Fundraising is a key element for most charities. In this context, one recurring question concerns the conditions under which a charity may conduct a fundraising and/or marketing campaign, by reaching out via email, post mail or phone to potential donors (both past and new donors) [39]. A related topic is whether a charity may research information on potential donors, use publicly available information and create potential donor profiles (on this issue, see also Section 6 below) [40].

The safe answer to these questions is: get consent [41].Obviously, if charities may rely on consent of the data subjects for their fundraising and marketing activities, they will be on the safe(st) side. In practice, this raises some issues, however:

→ First, in a charity-donor relationship, it is obviously delicate to request consent for processing personal data to someone who has just given some of his money to a charity.
→ Second, if a charity wishes to extend its population of donors, proceed to explanatory research in this field, or reach out to potential new donors, as a matter of fact, it will not have the prior consent of such prospects.

Considering these issues, charities support in some occasions, where consent is missing, that they may process data based on their legitimate interest.

In this respect, it should first be noted that legitimate interest implies that a due diligence assessment be performed. This assessment (also referred to as the 3-step legitimate interest assessment, "LIA": purpose, necessity and balance) [42] includes notably the necessity to balance the interests of the data controller (i.e. here, the charity) or a relevant third party, against the rights of data subjects [43].

The main downside of legitimate interest over consent is that it relies on one's own assessment, with no guarantee that an authority would share the outcome of the assessment.

In relation to charities, the GDPR (and more particularly its Recitals) does not contain any mention according to which charities would be entitled, because of their particular nature, to rely more than for-profit entities on legitimate interest in order to justify the processing of personal data in relation to their funding and marketing activities.

Interestingly, the Information Commissioner's Office of the United Kingdom addressed this specific issue and provided for a dedicated course of action to be observed:

"A charity wants to send fundraising material by post to individuals who have donated to them in the past but have not previously objected to receiving marketing material from them. The charity's purpose of direct marketing to seek funds to further its cause is a legitimate interest. The charity then looks at whether sending the mailing is necessary for its fundraising purpose. It decides that it is necessary to process contact details for this purpose, and that the mailing is a proportionate way of approaching individuals for donations. The charity considers the balancing test and takes into account that the nature of the data being processed is names and addresses only, and that it would be reasonable for these individuals to expect that they may receive marketing material by post given their previous relationship. The charity determines that the impact of a fundraising mailing on these individuals is likely to be minimal; however, it includes details in the mailing (and each subsequent one) about how individuals can opt out of receiving postal marketing in future" [44].

In our view, there are two main takeaways to be drawn from this guidance:
→ First, the UK Data Protection Authority does not exclude the fact that a charity may rely on its legitimate interest to conduct funding and marketing campaigns. On another hand, this authority does not say that legitimate interest may be a sufficient ground in any given instance. As a result, one may conclude that this has to be determined on a case by case basis.
→ Second, the UK Data Protection Authority addresses the case in which a charity is dealing with data of previous donors. It does not address the question of whether a charity could reach out to new potential donors, with whom it has never had contacts before [45]. With no doubts, the balance of interests in favor of the charity would be more difficult here, and one might have to wait until a Court decides on the legality of such activity under the GDPR to reach more legal certainty.

Lastly, besides the GDPR, soliciting (potential) donors by electronic means such as e-mails or sending e-mail newsletters falls under the scope of the ePrivacy Directive referred to in Section 2 above. This regulation requires prior consent to email communications. Thus, the ePrivacy Directive adds another layer of obligations on charities (and other entities alike) [46]. Similarly, Article 3 para. 1(o) of the Federal Act against Unfair Competition [47] prohibits spamming activities.

4.4 Other activities of charities involving data. In addition to the typical activities addressed above, charities carry out many other activities involving the processing of personal data, such as organizing congresses, courses and seminars. While it cannot be excluded that in some specific circumstances the very nature of charities might justify the application of a somewhat more lenient treatment of these activities from a data protection perspective, this should as a matter of principle not be the case. Indeed, it does not seem that disregarding the right to self-determination of the individuals whose data are processed and the related safeguards set out in the GDPR in relation thereto may be justified only based on the fact that charities do not have a for-profit purpose. As a consequence, all developments under data protection law relating to the activities of for-profit entities are likely to be also relevant for charities.

5. GDPR AND INTERNATIONAL ORGANIZATIONS

While this may be surprising at first glance, the GDPR contains 75 entries for the words "international organizations".

The GDPR defines an international organization (IO) as an "organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries" [48]. Thus, the GDPR "seems to equate IOs with third countries as entities that are subject to a body of law other than EU law" [49].

The intersection between the GDPR and IOs is a complex (and to some extent also, political) issue.

The first question that arises in this respect is whether the GDPR applies to IOs. The ICRC Handbook takes position as follows: "International Organizations enjoy privileges and immunities to ensure they can perform the mandate attributed to them by the international community under international law in full independence and are not covered by the jurisdiction of the countries in which they work. They can therefore process Personal Data according to their own rules, subject to the internal monitoring and enforcement of their own compliance systems; in this regard they constitute their own "jurisdiction" [50]. In short, the GDPR would at first sight not to apply, *per se,* to IOs.

Thus, although the GDPR has its own material and territorial scope (see Section 3 above), its applicability to IOs primarily depends on the privileges and immunities of the concerned IOs and on the IO's status of international law in the EU legal order [51]. In this connection, it should be noted that the relations between the EU and the IOs are defined by either formal or informal agreements, by exchange of letters or by setting up certain practices [52].

Second, even if most IOs are of the view that the GDPR does not apply to them, they often unilaterally decide to comply with the GDPR, as it has turned out that it is not viable for them otherwise (this may be the main takeaway for charities), in particular for the following reasons:

→ Transfer of data to IOs: IOs receiving data from EU based sources cannot ignore the GDPR, given that Article 44 GDPR requires that transfers of personal data to IOs shall comply with the GDPR. In their day-to-day operations, IOs interact with other entities which are subject to the GDPR and have to comply with all obligations set out in this piece of regulation, in particular when they enter into agreements with third parties (including IOs) comprising the processing of personal data.

→ Reputation: As a "force for good", IOs generally acknowledge the importance of this body of law, as well as the necessity for them to be able to offer a similar level of protection of data. From a reputational perspective, it would therefore be difficult for IOs to argue that they do not follow the best standards relating to the protection of individuals, including in the field of data protection.

As a last note, the above rationale also applies to UN agencies. For these reasons, some of these agencies have already adopted comprehensive internal privacy policies, which are largely compliant with GDPR standards [53].

6. SANCTIONS AND REGULATORS ACTIONS AGAINST CHARITIES

One of the reasons for which the GDPR has attracted much attention around the world is the sophisticated and heavy regime of sanctions that has been embodied into this piece of legislation. This regime has been inspired by the rules existing now for decades in competition law and which have largely contributed to the effective implementation of and, respectively, compliance with this field of law. In short, under the GDPR, fines may be imposed up to EUR 20 million or, in the case of an undertaking, 4% of its total worldwide annual turnover [54]. Even if the GDPR speaks of administrative fines, such fines may reasonably qualify as sanctions of quasi-criminal nature [55].

Addressing the whole regime governing sanctions under the GDPR would obviously go beyond the scope of this paper. Therefore, we will limit our developments to the following three issues:

→ First, sanctioning charities is not a theoretical question; it happens in practice. Cases in the UK even before the entry into force of the GDPR include, for instance, Battersea Dog's and Cats' Home upon which a fine of £ 9 000 was imposed for tele-matching, i.e., using personal data to obtain and use telephone numbers which data subjects may have chosen not to provide to the data controller [56], and Cancer Research UK, upon which a fine of £ 16 000 was imposed for notably using the services of a wealth screening company to analyze the financial capacity of its supporters in order to identify those that would have the means and propensity to make a larger donation to the charity [57]. While these amounts remain relatively modest, one should take into consideration that those charities were also indirectly sanctioned through the publication of the decisions handed down by the ICO, which affects their reputation.

→ Second, one could be tempted to argue that charities do not realize any turnover and therefore that no sanction based on any turnover could be imposed on such entities. Even though it is true that some charities do not realize any turnover, some other charities have a commercial activity in order to serve their public-interest purpose and thus do realize a turnover. Moreover, it cannot be excluded that the funds received by charities (donations, subsidies, etc.) qualify as turnover within the meaning of data protection law. Last, and as indicated above, turnover is not the only parameter based on which fines can be imposed; fines can go up to EUR 20 million regardless of any turnover.

→ Third, the first sanctions based on the GDPR have been recently imposed, and some lessons may be learned from these cases. In Portugal, for instance, a hospital was heavily fined (EUR 400 000) for, among other reasons, not setting up a proper access right policy, which led to an overly broad access to medical records by employees of the hospital [58]. Such an issue is relevant for many charities, and in particular, for several charities in the humanitarian field which have access to sensitive data relating to people in war zones or being in precarious situations.

7. CONCLUSION: WHAT CHARITIES SHOULD DO

It results from the above that the GDPR considers, to some extent, the unique nature of charities and IOs. This is evidenced by some Recitals of the GDPR and the guidance provided by data protection authorities as to its application.

That said, this does not mean that the GDPR is not applicable to Swiss-based charities. On the contrary, such entities can, in our view, not ignore this piece of regulation, and they must take necessary steps to ensure compliance therewith. In short, this means notably (i) mapping the data held by the charity and understanding the data flows, (ii) adopting the appropriate policies (e.g. data retention policy, data breach policy, policies governing the use of technologies), (iii) verifying and, as the case may be, adapting internal processes, (iv) verifying and, if need be, adapting the contractual agreements with employees and third parties (including consultants), and (v) training staff.

While implementing such compliance measures, charities may obviously rely on resources available, such as for instance the Guidelines issued by Swissfoundations on the application of the GDPR in the non-profit sector [59]. ■

Footnotes: 1) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88). On this topic, see also, for instance, Frankl Philippa, A mix of junk and important stuff': how we sorted out our charity data for GDPR, The Guardian, 9 April 2018. **2)** GDPR, Recital 4. **3)** GDPR, Recital 1. **4)** GDPR, Article 4(1). **5)** See for instance the judgment of the EU Court of Justice of 19 October 2016, Patrick Breyer c/Bundesrepublik Deutschland (C-582/14). **6)** GDPR, Article 5(1)(a) and Article 6(1). See also Filippidis Mariel, European Data Protection, Law and Practice, IAPP Publication, 2018, p. 99. **7)** GDPR, Article 5(1)(b). See also Filippidis Mariel, European Data Protection, Law and Practice, IAPP Publication, 2018, p. 104. **8)** Guidance provided by the UK Information Commissioner's Office (ICO) at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (last consulted on 12 January 2019). **9)** GDPR, Article 5(1)(c). See also Filippidis Mariel, European Data Protection, Law and Practice, IAPP Publication, 2018, p. 106. **10)** Guidance provided by the UK ICO (supra 8). **11)** GDPR, Article 5(1)(d). See also Filippidis Mariel, European Data Protection, Law and Practice, IAPP Publication, 2018, p. 107. **12)** Guidance provided by the UK ICO (supra 8). See also Filippidis Mariel, European Data Protection, Law and Practice, IAPP Publication, 2018, p. 108. **13)** GDPR, Article 5(1)(e). See also Filippidis Mariel, European Data Protection, Law and Practice, IAPP Publication, 2018, p. 108. **14)** Guidance provided by the UK ICO (supra 8). **15)** GDPR, Article 5(1)(f). See also Filippidis Mariel, European Data Protection, Law and Practice, IAPP Publication, 2018, p. 109. **16)** GDPR, Article 5(2); GDPR Recitals 39 and 74. See also Pothos Mary, European Data Protection, Law and Practice, IAPP Publication, 2018, p. 195 seq. **17)** Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37–47). **18)** RS/SR 235.1. **19)** See the information provided by the Federal Office for Justice at https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html (last consulted on 12 January 2019). **20)** See the information provided by the National Council at https://www.parlament.ch/centers/documents/de/sitzungsplanung-spk-n.pdf (last consulted on 12 January 2019). **21)** GDPR, Article 3(1). **22)** GDPR, Article 3(2)(a). **23)** GDPR, Article 3(2)(b). **24)** The website of the European Data Protection Board is available at https://edpb.europa.eu (last consulted on 12 January 2019). **25)** The Guidelines on the territorial scope of the GDPR issued by the EDPB are available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf (last consulted on 12 January 2019). **26)** The Guidelines on the application of the GDPR issued by the Swiss Federal Data Protection and Information Commissioner (entitled Le RGPD et ses conséquences sur la Suisse) are available at https://www.edoeb.admin.ch/edoeb/fr/home/documentation/bases-legales/Datenschutz%20-%20International/DSGVO.html (last consulted on 18 January 2019). **27)** EDPB Guidelines (supra 25), p. 5. **28)** In the same direction, see the Swiss Federal Data Protection and Information Commissioner's Guidelines (supra 26), p. 4. **29)** EDPB Guidelines (supra 25), p. 5. **30)** Swiss Federal Data Protection and Information Commissioner's Guidelines (supra 26), p. 4. **31)** EDPB Guidelines (supra 25), p. 15. **32)** Martinier Stéphanie, Does the GDPR Impact How Charitable Organizations Solicit Donors?, The Proskauer corporate social responsibility and pro bono blog, 4 December 2018, available at www.proskauerforgood.com (last consulted on 12 January 2019). **33)** EDPB Guidelines (supra 25), p. 18. **34)** Consent must be given «by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her» (GDPR, Article 7). **35)** Kuner Christopher and Marelli Massimo (editors), Handbook on Data Protection in Humanitarian, available at https://shop.icrc.org/e-books/handbook-on-data-protection-in-humanitarian-action.html (last consulted on 12 January 2019). **36)** Recital 46 must be read in connection with Recital 112 on transfer of data to international humanitarian organization, as well as the relevant provisions of the GDPR strictly speaking, it being specified that they do not expressly refer to humanitarian activities. Those provisions are Article 6(1)(d) GDPR («Processing shall be lawful only if and to the extent that at least one of the following applies: [...] processing is necessary in order to protect the vital interests of the data subject or of another natural person») and Article 9(2)(c) GDPR (regarding processing of special categories of data where «necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent»). **37)** GDPR, Article 5(1)(a). **38)** GDPR, Article 5(1)(f). **39)** The UK Information Commissioner's Office (ICO) published a guide on Direct Marketing (Data Protection Act and Privacy and Electronic Communications Regulations) which contains relevant research and guidance on this topic. This document is available at https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf (last consulted on 12 January 2019). **40)** For a good overview from a regulator's perspective, see the dedicated page of the UK Information Commissioner's Office (ICO): https://ico.org.uk/for-organisations/charity/. Other useful resources: General Data Protection Regulation, A guide for Charities, published by Charity Finance Group, 2018 (Authors: Buzzacott, Crowe Clark Whitehill, Kingston Smith); Data Protection, A guide for charities and non-governmental organisations, published by Thomson Reuters Foundation, June 2018 (Authors: CMS, Duncan Turner, Joy Black, Claire Brown; Dentsu Aegis Network, Mahisha Rupan, Hannah Wilkinson; Thomson Reuters, Erika Hayes). **41)** GDPR, Article 7. **42)** Guidance provided by the UK Information Commissioner's Office (ICO) at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ (last consulted on 24 January 2019). **43)** Data Protection Network, Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation, v 2.0, 6 April 2018, available at https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance. Recitals of the GDPR provide examples of processing that could be necessary for the legitimate interest of a Data Controller. Particularly relevant for charities in this context is Recital 47 «processing for direct marketing purposes». **44)** Guidance provided by the UK Information Commissioner's Office (ICO) at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/ (last consulted on 24 January 2019). **45)** The UK Information Commissioner's Office (ICO) gives some further insights on this: "For example, although marketing may in general be a legitimate purpose, sending spam emails in breach of electronic marketing rules is not legitimate", available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/; (last consulted on 12 January 2019). **46)** Martinier Stéphanie, Does the GDPR Impact How Charitable Organizations Solicit Donors?, The Proskauer corporate social responsibility and pro bono blog, 4 December 2018, available at www.proskauerforgood.com (last consulted on 12 January 2019). **47)** RS/SR 241. **48)** GDPR, Article 4(26). See also Kuner Christopher, International Organizations and the EU General Data Protection Regulation, University of Cambridge Faculty of Law, Paper No. 20/2018, February 2018, p. 10. **49)** Kuner Christopher, International Organizations and the EU General Data Protection Regulation, University of Cambridge Faculty of Law, Paper No. 20/2018, February 2018, p. 12. **50)** Kuner Christopher and Marelli Massimo (editors), Handbook on Data Protection in Humanitarian (supra 35), p. 24. **51)** Kuner Christopher, International Organizations and the EU General Data Protection Regulation, University of Cambridge Faculty of Law, Paper No. 20/2018, February 2018, p. 13. **52)** Kuner Christopher, International Organizations and the EU General Data Protection Regulation, University of Cambridge Faculty of Law, Paper No. 20/2018, February 2018, p. 19. **53)** See for instance IOM, available at http://publications.iom.int/books/iom-data-protection-manual (last consulted on 12 January 2019); UNHCR, available at https://data2.unhcr.org/en/documents/download/44570 (last consulted on 12 January 2019). **54)** GDPR, Article 83(5). **55)** See in particular the judgment of the Federal Tribunal of 29 June 2012 (ATF/BGE 139 I 72). **56)** Decision of the UK Information Commissioner's Office (ICO) of 3 April 2017 (Battersea Dogs's and Cat's Home), available at https://ico.org.uk/media/action-weve-taken/mpns/2013885/battersea-dogs-and-cats-home-monetary-penalty-notice.pdf (last consulted on 12 January 2019). **57)** Decision of the UK Information Commissioner's Office (ICO) of 3 April 2017 (Cancer Research UK), available at https://ico.org.uk/media/action-weve-taken/mpns/2013883/cancer-research-uk-monetary-penalty-notice.pdf (last consulted on 12 January 2019). **58)** The summary of this case is available at https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/ (last consulted on 12 January 2019). **59)** Swiss-Foundations, La nouvelle législation suisse en matière de protection des données – ce qu'il faut observer, Des outils pratiques rédigés par des praticiens, Circulaire SwissFoundations, November 2018.