NCHS PAPER

10 | APRIL 2023

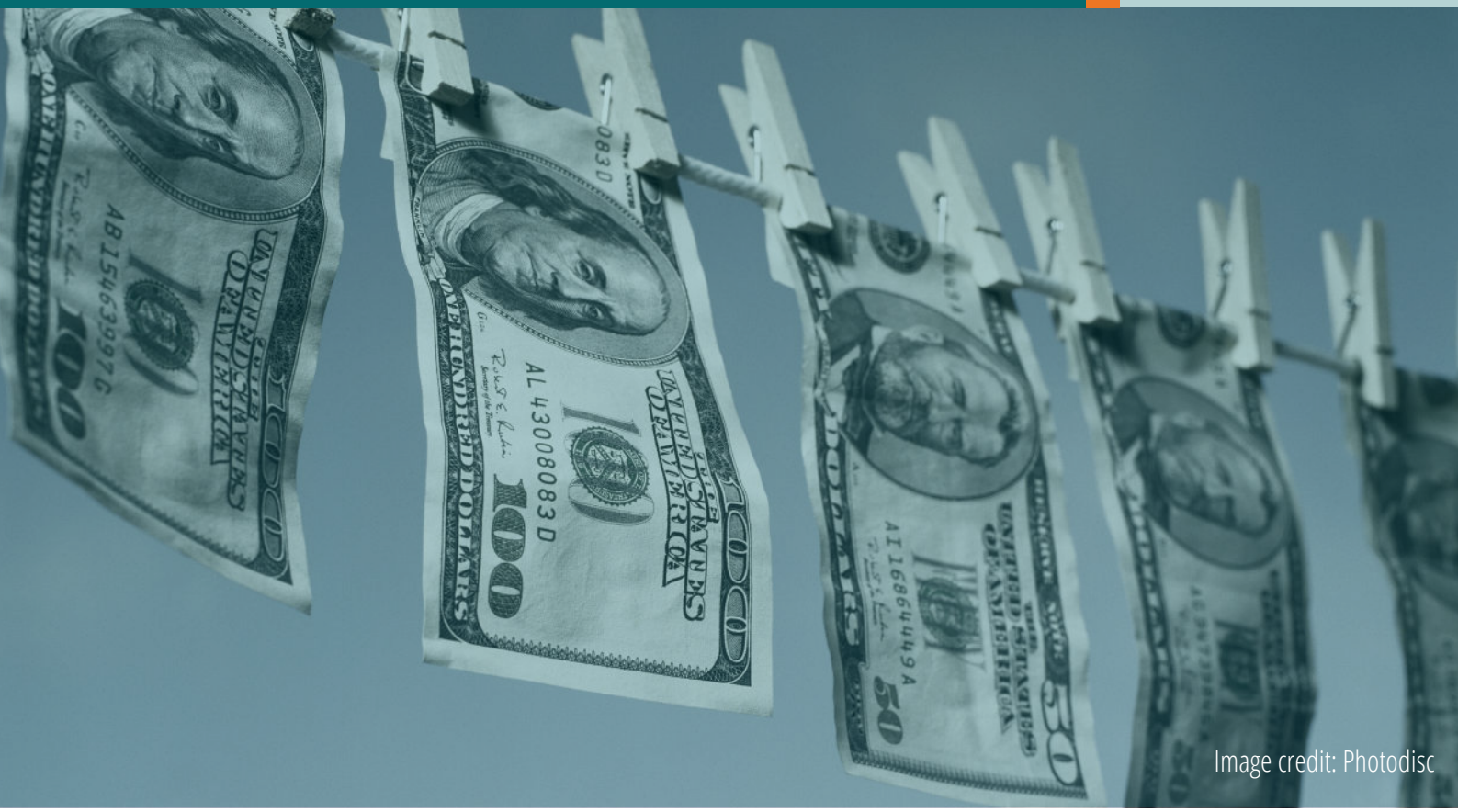

Image credit: Photodisc

OPACITY OR TRANSPARENCY? SCREENING BY NGOS IN THE CONTEXT OF AID WORK

NGOs delivering aid are often required to screen individuals against various watchlists to prevent terrorism financing and money laundering. This NCHS paper explores how European NGOs communicate the act of screening to the public and associated transparency implications.

AUTHOR

Beata Paragi
Associate Professor,
Corvinus University

Thousands of international non-governmental organisations (hereinafter INGOs or NGOs)[1] operate in the Global South with the aim of providing development assistance, humanitarian aid or doing advocacy work for the benefit of less privileged populations. Aid work, however, is not free of real or perceived security risks. National legislative bodies (HRC 2019), banks and financial service providers (FATF 2015), and donors equally demand that INGOs prevent terrorism financing and money laundering through different structures and mechanisms engrained in law, related regulations and guidelines (Hayes 2012; Hayes 2017). As a result, NGOs working with official donors (the United States government, the European Union (EU) or national aid agencies of member states) cannot but sign funding agreements with conditional clauses (NRC, 2018a; NRC 2018b). While these conditional clauses aim to prevent money transfers that might be used for financing terrorism or other illicit purposes in the Global South, measures of risk mitigation – such as screening – have been increasingly digitalised by larger, international NGOs.

Screening[2] refers to a procedure whereby INGOs implementing aid projects in the Global South check the background of individuals against various watchlists in order to comply with international and domestic (sanctions) law, with conditional clauses enshrined in funding agreements or to pursue other organisational interests.

Screening against various watch lists and the use of tech solutions raise questions with regards to the law and politics of listing (de Goede and Sullivan 2016; Minnella 2019; Sullivan 2020), the nexus of IR, mainstream and critical terrorism and security studies (Federer 2022), and human rights and data protection law (Tzanou, 2017). While screening has been problematised by practitioners as screening of final beneficiaries is at odds with humanitarian principles (Gillard 2021a; Gillard 2021b), its data protection dimension is not only less exposed, but it also means a huge challenge to aid organisations (VOICE 2021, 3).

As the principle of transparency and the right to information are key elements of contemporary data protection legislations (Klareen, 2013; Vrabec 2021), the purpose of this paper[3] is to explore how European NGOs communicate the act of screening to the public. Conceptualising screening as a data processing operation, the paper communicates some findings of a research project (Paragi, 2022), the original aim of which was to explore NGOs' experiences and dilemmas with the EUs General Data Protection Regulation 2016/679 (GDPR). Sources selected for analysis equally included legal instruments and academic sources in the field of law and social science.

To address the matter of transparency the analysis equally builds on its contemporary conceptualisations and legal understandings. Transparency as an idea or concept, is related to but not identical to, transparency as a legal principle enshrined in legal instruments (Adams 2020). The difference matters to the extent which, transparency around screening may be expected from NGOs, even if it may vary from jurisdiction to jurisdiction how transparency can be restricted in the name of national security or international counterterrorism activities.

Transparency, as a principle and idea, encompasses equality and balance of power both in public and private contexts serving the objectives of legitimate governance (Vrabec 2021, 65). It has been recognised as a legal principle by nations over the past decades, the purpose of which has been to equip citizens with the right to know in order to strengthen democracy (Schudson 2018) and theright to (access to) information. Due to rapid digitalisation and the widespread application of technologies performing automated decision-making or using artificial intelligence, the emerging 'right to be explained' joined the right to information (Kaminski 2019), both strongly communicating with the legal principle of transparency.

With regards to EU/EEA jurisdictions, the core instrument regulating data protection, and as part of that, the principle of transparency and related right to information, is the GDPR. Being a regulation, it has general application and as such it is binding in its entirety and directly applicable in all Member States. Its status implies that the principles listed in Article 5 – transparency included – are also legally binding. In addition to the regulation itself, recitals in the preamble of the GDPR were also used for analysis. While recitals in EU law do not constitute the rule itself, they elaborate on the reasons for the operative provisions avoiding normative language and political argumentation. Guidelines issued by the European Data Protection Board (EDPB) or its predecessor (Article 29 Working Party) were also selected and scrutinised for relevant content. They detail the GDPR's territorial scope (EDPB 3/2018); transparency (Article 29 WP 2018) and data subject's rights: access to information (EDPB 1/2022).

The analysis of legal sources was complemented with an overview of publicly available privacy notices (PNs), semi-structured qualitative interviews with NGO officers (n=12, in 2021) and a workshop held at Peace Research Institute (PRIO), Oslo in 2022. As for the PNs, NGOs were selected based on their VOICE-membership (n=88) and also on a random basis (n=5) so that larger actors being present in multiple areas, with a diverse profile and employee pool should be part of the sample. All in all, 92 publicly available privacy notices[4] were checked in November 2022 looking for evidence of screening under sub-themes, such as purposes of processing and data transfer to third parties. Terms such as (ethical) screening, vetting, background check, due diligence, fraud prevention, AML/CFT (anti-money laundering, combatting the financing of terrorism) were deemed 'direct' evidence, but indirect formulation also considered the extent to which screening may have been inferred from other wording. While the interviews concerned GDPR-compliance in general, the workshop had a narrower purpose, namely, discussing the data protection dimension of screening with practitioners. As for the workshop, participants included researchers (n=7), legal advisors and Data Protection Officers (DPOs) (n=11) of aid organisations (n=6).[5] Quotes are used only to illustrate typical dilemmas international NGOs face.

This paper unfolds the following way. Elaborating on the essence of screening and the scope of the problem in section 1, followed by a brief summary of the context of screening focusing on conditional clauses and the applicability of the GDPR in section 2. The principle of transparency is discussed in section 3 and section 4 summarises NGOs conduct. The circumstances under which restrictions or exemptions may apply is discussed in section 6, followed by a short conclusion.

1. SCREENING

Screening, if done manually, requires a lot of work. As legal-regulatory requirements of international and domestic sanctions law have become increasingly complex, commercial actors have started to consolidate the different lists into searchable products by offering digitalised solutions to their customers. These products and services were originally developed for or by financial service providers (FSPs) being under legal obligation to implement customer due diligence procedures, such as know-your-customer (De Goede and Sullivan 2016; Shabibi and Bryant 2016).

Screening in practice is about running a search online, among others, that is, checking whether lists of personal data match various watchlists in the consolidated database. The most popular tech solutions available on the market are FinScan, LexisNexis (former WorldCompliance), CSI WatchDOG Elite, Bridger Insight Online, Visual Compliance System (VOICE 2021, 13) and World-Check from Thomson Reuters (De Goede and Sullivan 2016). These tools enable users, NGOs included, to synchronise watchlist screening and navigate continuously shifting sanctions, financial crime compliance and anti-bribery requirements. Regardless of service providers and legal frameworks of data protection, screening implies users' access to results of "a thorough sequence of research, vetting and data compilation … provide[d in] robust databases of high-risk individuals and entities" (LexisNexis® WorldCompliance™).

Screening as a data processing operation: This description above corresponds to terms used in GDPR Article 4(2) and in Court of Justice of the European Union (CJEU) jurisprudence to describe processing operations, such as collection, recording, structuring, storage, retrieval, consultation, use, disclosure and loading personal data[6] on an internet page.

While searches may be run occasionally or regularly, these databases are cloud-based, multiple and integrated. Screening can also be considered a data processing operation to the extent to which personal data is shared with the service provider during a search to check if lists of personal data (of natural persons) match various watch lists in a consolidated database or when NGOs store results of screening for compliance purposes.

The scope of the problem: Screening implies that the personal data of *any* individual getting in direct touch with NGOs can be processed either manually or in automated ways when they are deemed to pose financial, legal or reputational risk. Acknowledging that considerable opacity prevails around screening, only estimations are available regarding the scope of the problem (VOICE 2021, 13). To approximate the size of the problem in quantitative terms, only a few sources can be cited. For example, the Norwegian Refugee Council conducted 7,053 searches for screening partner staff, suppliers and employees only in the Middle East in 2018 (Charny 2019). It may be reasonably inferred that international NGOs with thousands of employees, transactions and beneficiaries run tens of thousands of searches each year which follows (from) the business models of the commercial actors supplying the product. This amount may even be considered 'large scale' data processing operations, and as such, poses high risk for data subjects' rights.[7]

2.THE CONTEXT OF SCREENING: COUNTERING TERRORISM AND PROTECTING PERSONAL DATA

Countering terrorism: Conditional clauses in funding agreements

The contemporary obsession with security coupled with domestic and international legislation on counterterrorism, sanctions, national and/or public security implies that operations and transactions of non-security actors have been increasingly securitised from the financial sector through the telecommunication industry to airlines (De Goede 2018). Financial transactions of NGOs, are not exceptions either (Watson and Burles 2018). In addition to legal obligations, conditional clauses in funding agreements also push these organisations to automatise screening to remain eligible for future tenders.

Taking the EU as an example, in the context of aid projects financed by the European Commission (EC) either via the DG International Partnerships (DG INTPA) or by the DG in charge of humanitarian support (DG ECHO), actors implementing EU-financed projects may sign two main types of contracts – grant agreements or service contracts – depending on the activity to be financed from the EU budget. Both types of contracts contain references to preventive measures, a matter that has direct implications in the context of personal data protection for the personal data involved, collected and processed by NGOs.

Considering development NGOs, DG INTPA introduced the counter-terrorism clause in its contracts with (development) NGOs from Summer 2019 with the purpose of ensuring that no funding is made available to designated terrorist organisations. As a result, Annex II to the current grant agreement[8] (to be signed by NGOs in cases of projects managed by DG INTPA) reads as follows:

> 12.2. … in the following circumstances the contracting authority may … terminate this contract or the participation of any beneficiary(ies) in this contract without any indemnity on its part when (d) it has been established by a final judgment or a final administrative decision or by proof in possession of the contracting authority that the beneficiary(ies) has been guilty of … money laundering or terrorist financing, terrorist related offences.

And with regards to the measures expected from NGOs implementing projects with financial support from the EU:

> 1.5.bis [g]rant beneficiaries and contractors must ensure that there is no detection of subcontractors, natural persons, including participants to workshops and/or trainings and recipients of financial support to third parties, in the lists of EU restrictive measures.

Acknowledging that delimitation is not always clear cut, it is important to distinguish development NGOs from humanitarian NGOs, the latter operating in line with the humanitarian principles. Considering the mandate of the latter, the DG ECHO included a text in its grant agreement excluding the vetting of final beneficiaries (in 2021): “the need to ensure the respect for EU restrictive measures must not however impede the effective delivery of humanitarian assistance to persons in need in accordance with the humanitarian principles and international humanitarian law. Persons in need must therefore not be vetted” (Annex 5 of the Humanitarian Aid grant agreement).

To clarify the rules, the European Commission published the *Commission guidance note on the provision of humanitarian aid in compliance with EU restrictive measures* in 30 June 2022 according to which (p 11):

> Funds and economic resources cannot be provided to designated persons either directly or indirectly, unless those persons qualify as persons in need of humanitarian aid.

International funding policies equally imply that all other individuals and entities – staff, partners, suppliers, individual donors – will continue to be required to be screened even by humanitarian NGOs, just as beneficiaries of development aid projects channelled through DG INTPA. While a recently adopted UN Resolution (UNSC 2664/2022) permits "the payment of funds, other financial assets, or economic resources, or the provision of goods and services necessary to ensure the timely delivery of humanitarian assistance" without considering it the "violation of the asset freezes imposed by this Council or its Sanctions Committees," paragraph 3 of the resolution prompts that the exemption does not apply to the expected risk-mitigation measures. Indeed, the Security Council keeps requesting "[humanitarian] providers … to use reasonable efforts to minimise the accrual of any benefits prohibited by sanctions, … by strengthening risk management and due diligence strategies and processes."

Interpreting sanction clauses in grant agreements is not easy in practice, especially in cases of organisations working in conflict situations (NRC 2018b). For example, as demonstrated by Palestinian concerns (BADIL 2021), it was unclear for the local NGO community whether the obligation formulated in the EU 1.5.bis article "applies towards natural persons who are not listed but are a part of [terrorist] organisation [listed on the EU restrictive measures list], either formally or informally." Hence, if an NGO is a beneficiary of an EU grant contract, a broad interpretation of the clause may lead to the termination of the contract (BADIL 2021).

The matter of compliance is further complicated if the US is involved as a donor in any of the operations of an NGO for it demands that recipient NGOs sign the ATC (anti-terrorism certificate) with the following content (cited by Eckert 2022):

> The Recipient, to the best of its current knowledge, did not provide, within the previous ten years, and will take all reasonable steps to ensure that it does not and will not knowingly provide, material support or resources to any individual or entity that commits, attempts to commit, advocates, facilitates, or participates in terrorist acts, or has committed, attempted to commit, facilitated, or participated in terrorist acts.

This definition interprets the category of 'terrorist' much more broadly than sanctions laws usually do, and prompts that NGOs are required to screen not only against lists containing the names of designated individuals (and entities) – but basically anyone that fits the US' interpretation.

European aid NGOs in the Global South and the scope of the GDPR

Reflecting the importance it attributes to the protection of fundamental rights, the GDPR not only applies within the EU, but is also extended to the EU's external trade – and aid – relationships for its territorial scope (Bennett 2018; Schmidt 2022, 246). European NGOs, even if they implement projects in the Global South are bound by the GDPR (Gazi 2020; Paragi 2020; Franz et al 2020) as long as their data processing operations fall under the scope of the GDPR.

The GDPR is the first data protection law to make specific reference, however vaguely, to humanitarian action: 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 (Recital 46); with regards to restrictions they can be imposed to protect the rights and freedoms of others, including social protection, public health and humanitarian purposes (Recital 73); and referring to data transfers to international organisations in humanitarian context (Recital 112) (Kuner and Marelli 2020).

With reference to its territorial scope, Article 3(a) of the GDPR states that "the regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not" (GDPR). The global significance of this article made the EDPB issue guidelines on the meaning of 'territorial scope' (EDPB 3/2018, 10) interpreting Article 3(a) in the following way:

> [A]ny personal data processing in the context of the activities of an establishment of a controller or processor in the Union would fall under the scope of the GDPR, regardless of the location or the nationality of the data subject whose personal data are being processed.

This approach is strengthened by Recital 14, which states that "[t]he protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data" (EDPB 3/2018, 10).

This implies that aid organisations (NGOs, business organisations or public agencies) that are registered within the EU/EEA but operate outside its borders (implementing aid projects, delivering services and related processing activities) are regulated by the GDPR. In other words, the GDPR applies even if an EU-based NGO processes the personal data of non-EU citizens and/or if it operates in the Global South[9] (Gazi 2020; Paragi 2020; Franz et al 2020).

With regards to the material scope, as Article 2(1) says, the GDPR "applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." Article 2(2) lists exceptions when the GDPR does not apply, namely, when the course of an activity (and related data processing operations) fall outside the scope of the Union law; when personal data is processed by Member States when carrying out activities in the context of provisions concerning the common foreign and security policy (the scope of Chapter 2 of Title V of the TEU); when personal data is processed by natural persons "in the course of a purely personal or household activity" and last but not least when competent authorities process personal data for the purposes of "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security." Considering these exceptions, it should be noted that NGOs are legal entities (not natural persons) and not authorities in charge of criminal investigations, national or public security issues – even if their work and operations have been securitised in the context of the global war on terror.

Aid organisations collect and process the personal data of various categories of data subjects. Employees, board members, volunteers, activists, beneficiaries of aid projects or services, suppliers and partners are equally natural persons whose personal data, processed by NGOs, can be used to identify (authenticate) them before a contract is signed, a transaction is made or a project is implemented. NGOs, however, may also use personal data to screen against sanctions and other watch lists. Citizenship does not make a difference: individuals in the Global South can be identified by their personal data (name, date of birth, etc.) the same way as if they hold EU passports in case of screening too.

To sum up, the digitalised activities of NGOs fall under the territorial and material scope of the GDPR to the extent which personal data is involved. With regards to the operation itself and considering the definition of processing (Article 4(2); Tosoni and Bygrave, 2020), if an NGO – for whatever purpose and on whatever legal basis – (i) shares personal data (a person's name, date and place of birth) with an external service provider (ii) to search for positive matches in a database containing consolidated watch lists, (iii) stores the results of search for a(n) (in)definite amount of time, and (iv) makes decisions based on the results, the given set of data processing operations (labelled simply as 'screening') falls within the scope of the GDPR.

3.THE PRINCIPLE OF TRANSPARENCY IN THE GDPR

The GDPR requires controllers to render data processing transparent to data subjects, as access and information rights represent integral components of privacy and other fundamental rights (Polčák 2018, 405). In other words, transparency is a precondition for exercising the right to information – just as the right to information is the precondition for exercising other rights enshrined in the GDPR (Vrabec 2021, 64).

If data subjects are not provided information on the fact and purposes of (potential) screening, they can neither raise questions and claim their rights, nor consider the consequences of this operation either. As the relationship between the data subjects and the NGO is voluntary (at least theoretically), the information provided to them is crucial. Individuals may or may not enter or remain in contractual (or other) relationship with the NGO if they are aware of being screened.

The meaning of transparency varies across disciplines entailing not only diverse interpretations, but also conflicting interests as screening illustrates. The general discourse implies that "transparency concerns the disclosure of information by a particular entity with the view to increasing visibility and accountability of this entity to a broader spectrum of persons and institutions" (Adams 2020, 5) and denotes the conditions "in which information about the priorities, intentions, capabilities and behaviour of powerful organisations is widely available to the global public" (Lord, 2006, 5 cited by Adams 2020, 5).

In the context of development and humanitarian assistance, transparency also reflects a consensus that more and higher-quality information about aid should have positive impacts on aid effectiveness under adverse conditions, such as corruption in aid recipient countries (Christensen et al, 2011). Indeed, transparency in principle, constrains the power of the remote 'agents' (state actors, policy-makers) by making more information available to the local 'principals' (the public, voters, citizens). As a result, principals – those benefiting from aid – are better positioned to ensure that processes deliver outcomes closer to their preferences (Christensen et al, 2011).

Principles governing data processing and protection are listed in GDPR Article 5. The six (seven) principles – (1) lawfulness, fairness, transparency; purpose limitation; data minimisation; data accuracy; storage limitation; integrity and confidentiality and (2) accountability (not discussed in this paper) – govern how personal data should be processed and protected by data controllers and processors.

Focusing only on the first set of overlapping principles presented in Article 5(1)a, it prescribes that personal data shall be processed "lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')." Lawfulness and fairness were also explicitly mentioned in earlier legislation concerning data protection (Directive 95/46/EC), and their meaning has not changed with the adoption of the GDPR in 2016. The third element in Article 5(1)a, transparency, however, is a new component, at least in the EU data protection framework, complementing the first two principles.

Looking at the components of Article 5(a) one by one, lawfulness of processing means that personal data can only be processed if authorised by law. In other words, those processing personal data are required to follow the GDPR (as a rule of thumb) for ensuring adequate data protection by selecting a lawful basis for processing (Article 6: consent obtained from the data subject; necessity to enter a contract; legal obligation; vital interests of the data subject; performing a task for public interest; legitimate interests of the controller or a third party).

Furthermore, data processing also needs to be in line with other EU legislation and domestic laws (at least constitutions). Rights enshrined in the GDPR can be restricted by taking into consideration that "the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights …" (Recital 4).

The fairness principle governs the relationship between the controller and the data subject by ensuring that processing operations are "not performed in secret" and data subjects are "aware of the potential risks" (EU Handbook, 2018, 118).[10] The principle of fairness already appeared in Directive 95/46/EC as the prohibition of secrecy and the requirement of comprehensive information. [11] It also implies that "natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing" (Recital 39 and 60). Furthermore, fairness also implies that "data controllers must take some account of the reasonable expectations of data subjects" which carries "direct consequences for the purposes" for which data may be processed (Bygrave 2014a, 146).

The third component, transparency, establishes, among others, an obligation for the controller to ensure that the data subjects are informed about how their data is used (Recital 39 and 60) and for what purposes their data is processed (EDPB 2/2019, 8). The application of this principle cannot be limited to a single event, a single act (providing certain information), a single piece of information or a particular means or form used for communicated information. The rationale behind transparency is to enable data subjects to understand, and if necessary, challenge those processes, by empowering data subjects to hold data controllers and processors accountable and to exercise control over their personal data (Article 29 WP, 2018, 4 and 5). As argued by the EDPB, transparency "empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent" (Article 29 WP, 2018, 5).

Regardless of the legal basis of a given data processing operation and for being a principle, transparency is prescribed, that is, to be applied in general – and not only in cases when the legal basis of processing is consent.

As implied, the relationship between transparency and fairness is two-way or mutual (Article 29 WP, 2018, 4). Fairness and transparency together concern the ways and method of communication (vis-a-vis the data subjects), and the content of the information. While fairness is about the provision of complete information by the data controller, transparency has more to do with the content and quality of the information. On the one hand, fairness may ensure transparency as a proportionality safeguard (Article 29 WP, 2018, 5), especially in cases of power imbalance between the controller and the data subject. On the other hand, 'fair processing means [implies] transparency of processing, especially vis-à-vis data subjects' by implying that 'data have not been obtained nor otherwise processed through unfair means, by deception or without the data subject's knowledge' (de Terwangne, 2018, 314). These principles explicitly appear in the articles describing data subjects' rights: "the controller shall … provide the data subject with the … information necessary to ensure *fair* and *transparent* processing (Article 13(2) and 14(2)).

The principle of transparency is supported and advanced by other elements in the GDPR. Rights of the data subjects are too complex to be discussed here comprehensively, but it should be noted that transparency encompasses all of them. Transparency with regards to data processing and data protection is proportional to the strengths of individual rights: more transparency entails stronger rights.

The most relevant legal content is detailed in GDPR Article 12, 13-14 and 15; Recitals 11, 58, 59, 60, 63, 166 (Polčák, 2018, 398-420). As formulated in Article 12(1):

> The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

While compliance with the transparency principle is a precondition for exercising rights, the right to information is also deemed to be the precondition for other rights enshrined in the GDPR. In the framework of data subject rights, Article 12 lays down the requirements for appropriate measures to be adopted by the controller when providing the information (in line with Article 13 and 14) and also for communications referred to in Article 15-22 and 34 GDPR. Without having general information on data processing operations, including personal data and/or access to specific information on data processing involving one's personal data – such as screening – there is no knowing and understanding which is further needed for claiming rights.

As far as the content and ways of communication (disclosing information about the essence of the use of data and related data processing operations) are concerned, the following main elements (of Article 13 and 14) require consideration by NGOs as data controllers as a minimum: the content of the information, the timing of providing information, the appropriate ways of providing information and the right to lodge a complaint as a minimum. The GDPR implies an obligation requiring the NGOs (data controllers) to comply with the transparency and fairness obligations proactively – unless restrictions or exceptions apply.

Privacy notices are not mentioned in the GDPR as a modality of communications, but transparency is listed among the rights of the data subjects (Article 12). Therefore, the privacy notice (data protection notice, privacy policy, privacy statement or fair processing notice) is seen as one of the most efficient measures to provide information (Article 29 WP 2018, 13) to data subjects – either on websites of organisations, or in alternative channels.

4.PRIVACY NOTICES IN PRACTICE: NGOS' CONDUCT

A comprehensive analysis of publicly available privacy notices was not the intention of this paper, but a few general comments can be made before notification with regards to screening is scrutinised. First, privacy notices of aid organisations are mostly addressed to European audiences – in national languages, sometimes with translations also available in English. The target audience comprises first and foremost of website visitors, social media users, newsletter subscribers (typical categories of data subjects addressed in almost all privacy notices), followed by individual donors, employees, volunteers, job applicants or candidates.[12] Transaction partners (suppliers, consultants) in the Global South and beneficiaries of aid programmes and projects are sometimes listed,[13] but it is not typical. An exceptionally clear reference to Global South individuals can be found in the privacy notice of *People in Need* (Czech Rep), which mentions 'data on aid recipients' as a separate (5.) category:

> In cases where we provide humanitarian aid to certain persons in the Czech Republic or abroad (in order to save lives, alleviate hardship and help victims of disasters or crises get back on their feet) or development aid (to help people in their efforts to break out of poverty and further develop) it is usually necessary in the interest of aid effectiveness, but also its reporting to donors to collect the personal data of aid recipients. The processing time is usually limited by the project implementation time and further by the time set by the donor or based on the nature of the specific project.

Privacy notices posted on NGO websites were primarily scrutinised to see if they contain any direct or indirect reference to screening. Findings indicate that screening as a processing operation in the publicly available privacy notice is invisible to the general public. EU-registered NGOs almost never communicate the practice of screening to data subjects.

Among the NGOs whose publicly available privacy notices were analysed for their content (in November 2022), only four privacy notices mentioned screening explicitly as a purpose of data collection: the (recruitment/employment) privacy notices of Norwegian Refugee Council (NRC) and PLAN UK; PLAN's general privacy notice and the privacy notice of the Croatian International Medical Corps (see Table 1). None of them linked the purpose of screening with a legal basis (Article 6(1)), but two of them made references to working with an external service provider.

International Medical Corps (IMC) Croatia	https://internationalmedicalcorps.hr/	To comply with anti-money laundering, terrorism and sanctions laws and regulations, there are times when we need to confirm (or reconfirm) the name, date of birth, address and other details of our donors and business partners (including their directors, officers, board members, owners, shareholders, authorised representatives and affiliates and their circumstances). We may need to do this whether you are applying to be a new donor or business partner or have been one for some time. This information may be shared with third-party service providers for this purpose.
Norwegian Refugee Council (NRC)	https://www.nrc.no/globalassets/graphics/nrcpeople/privacy-notice-for-recruitment.pdf	Privacy Notice addressed for employees (p1, footnote 1): "In accordance with core humanitarian principles, NRC implements a range of safeguards to *prevent or reduce the possibility of humanitarian aid falling into the wrong hands. This includes in particular those individuals and groups who are subject to sanctions imposed by the United Nations Security Council and other applicable sanctions lists*. As part of this process, *NRC may screen the details of the successful candidate for a position* against these sanctions lists."
Plan International UK	https://plan-uk.org/terms-conditions/privacy-notices	Privacy Notice addressed to employees: "it is necessary to carry out *criminal records checks* to ensure that individuals are permitted to undertake the role in question"; general PN: "5. Ethical *screening* … To do this we sometimes use profiling and *screening methods* so that we can better understand our supporters and potential supporters … we may carry out *background checks* … on donors and potential donors or check donations to help protect the charity from abuse, fraud and/or money laundering and/or terrorist financing".

Table 1: Privacy notices containing clear information on screening as of November 2022

Eight other organisations used a formulation which might be indicative of them collecting personal data for the purpose of screening, but the language is not clear and concise enough to draw conclusions. Considering the transparency principle and the notification obligations prescribed by the GDPR, a typical NGO would need to consider when drafting a privacy notice, among others, how personal data is involved in the case of screening, what screening means as a data processing operation; who defines the purposes of processing and, if data processors are used for conducting screening, what is the relationship between the controller and the processor, and which legitimate basis is used for screening.

The explanations for missing information on screening vary and require further research. However, it is worthwhile to recall that privacy notices are widely criticised both by data subjects and legal scholars for being unreadable and uninterpretable, for being too long, unstructured or too 'noisy' in terms of content in absence of proper standards (Becher and Benoliel, 2020). If privacy notices are not read, it is irrelevant – from the perspective of the non-reader – even if the information is provided in a manner that complies with the GDPR or scholarly advice. While the recent WhatsApp-decision of the Irish data protection authority (DPC 2021) established that privacy notices must be detailed – with far more detail being given than is currently typical – and must be easily accessible (without use of multiple linked documents, which may be hard to find and assimilate), it does not solve the problem of length. Those not reading – or being discouraged by purely seeing the length of any text – will not be helped by a well-structured text either.

Assuming that communication channels other than privacy notices posted on websites may also be a GDPR -friendly solution, guidelines on information provided orally can be considered relevant (Article 29 WP, 2018, 13):

> Where a data controller has chosen to provide information to a data subject orally, or a data subject requests the provision of oral information or communications, WP29's position is that the data controller should allow the *data subject to re-listen to pre-recorded messages*. This is imperative where the request for oral information relates to visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding information in written format.

No evidence confirms the use of pre-recorded messages by the sampled NGOs. A further problem with providing information orally is that it does not appear feasible considering the scope of screening. When tens of thousands of personal data records are screened on a weekly basis, when hundreds of new suppliers or employees are screened before the contract signed and later on, by the time contracts are terminated, providing information orally – in a concise, transparent, intelligible and easily accessible form and using clear and plain language – looks even more time-consuming than screening itself.

Regardless of the oral versus written form of notification, the concerned data subjects are rarely aware of the fact that their personal data, collected for purposes such as signing a contract or participating in an event, may also be checked against sanctions and enforcement lists, that is, disclosed to third parties.[14] As participants of the PRIO workshop agreed, even when minimum information is provided on screening (when signing a labour or supplier contract with a clause making references to screening), details are provided orally and in generic terms.

How information on screening is provided depends on the nature of the relationship between the NGO and the perceived (digital) literacy of the individuals, not so much on the documented legitimate basis. Those having a contractual relationship (employees and suppliers) or being in charge of money transfers over FATF (2016) standards are notified about screening when they sign their contracts. These contracts usually contain a clause making references to screening.

Those individuals whose relationship with NGOs are less regulated in legal terms (ie. there is no binding contract) are usually not provided with screening information.[15] Volunteers, consultants, beneficiaries of development projects or beneficiaries of CVA (cash and voucher) assistance (that may be screened as clients by the external financial service providers based on the lists provided by NGOs) in the Global South are usually not made aware of screening – regardless of how the legal basis (public interest, vital interest, legal obligation) may be documented by the NGO.

5.POSSIBLE RESTRICTIONS AND ALTERNATIVE WAYS OF COMMUNICATING SCREENING

Are NGOs allowed to withhold information on screening? Considering the distinction made between transparency as an idea and as a legal principle, there is no straightforward answer. It depends on how NGOs interpret transparency in light of national legislation, complementing the GDPR on the one hand and their own corporate image on the other hand.

As long as screening is a data processing operation, the GDPR applies. The regulation, however, allows certain exemptions and restrictions. Although a detailed discussion is not possible here, it should be noted that restrictions concerning *principles* – such as transparency, fairness, lawfulness prescribed by the GDPR – are strict. They are allowed only to the extent they (i) correspond with rights and obligations provided in Article 12 to 22 and (ii-1) only if exemptions and restrictions are provided for at EU or national level by law, (ii-2) pursue a legitimate aim and (ii-3) can be considered proportionate and necessary in a democratic society – at the same time (EU Handbook, 2018, 116). In line with this, Article 23 allows Member States (or the EU) to legislate for further restrictions on the scope of the data subjects' rights in relation to transparency and the substantive data subjects' rights provided that fundamental rights are not compromised, and restrictions are necessary and proportionate to safeguard one or more of the ten objectives set out in Article 23.1(a) to (j) (Article 29, 2018, 33).

Data subjects' rights – enshrined in the GDPR – are mostly restricted in the context of law enforcement and matters related to national security and counterterrorism by states or public authorities. The objectives and conditions justifying restrictions are listed in Article 23: national security; defence; public security; criminal prevention and enforcement; other important objectives of general public interest of the Union or of a Member State, e.g. financial or economic interests; the prevention, investigation, detection, and prosecution of breaches of ethics for regulated professions; a monitoring, inspection, or regulatory function connected, even occasionally, to the exercise of official authority in the cases referenced in points (a) to (e) and (g); and the protection of the data subject or the rights and freedoms of others.

Article 23(2) lists the provisions (subject to restrictions) which should be legislated, such as the purposes of processing, categories of personal data, the nature of restrictions etc. Recital 73 further specifies that restrictions may be imposed by Union or Member State law.

However, even if restrictions apply in some member states, "the domestic law must be sufficiently clear in its terms to give individuals an adequate indication of the circumstances and conditions under which controllers are empowered to resort to any such restrictions … and … it is indeed essential that legislative measures, which seek to restrict the scope of data subjects' rights or of controllers' obligations, are foreseeable for the data subjects" (EDPB 10/2020, 8). In other words, even if NGOs might be allowed to restrict data subjects' rights, individuals should understand the "circumstances in and conditions under" which controllers withhold information. Furthermore, there should be a legislative measure referred to in Article 23(1) containing specific provisions that prescribe or allow such restrictions: the controller is expected to inform data subjects that they are relying on such a national legislative restriction to the exercise of data subject rights, or to the transparency obligation in line with Article 23(2)h.

Recalling that transparency is not only a legal principle in the context of human rights and data protection law, but also a general idea that influences power relations, actors in the non-profit sector may consider the due diligence practices and strategies implemented by for-profit actors, such as banks (Helgesson and Mörth 2019). These practices not only include the collection and verification of client information (when a bank account is opened) and the monitoring of client transactions, but also the content and ways of communicating with clients about the AML/CFT measures implemented.

Taking the website of the Norwegian DNB as an example, the bank not only makes relevant information available on its website (here and here), but also a disclaimer stating that "the bank is neither an investigator nor a judge, but we monitor and report suspicious transactions to the police. In this area, we have a duty of confidentiality, which means that we do not inform our customers or others about what we do."

Obviously, the broader context in which aid NGOs work in the Global South, especially in humanitarian and conflict settings entail ethical questions beyond GDPR-compliance. An apparent challenge for NGOs is to navigate among their mission (providing assistance to vulnerable populations by considering not only human rights, but also local norms and values in a manner that does not undermine trust and their credibility), their mandate (ensuring that donor funds are processed within strict timeframes and in line with the project purposes) and other legal compliance requirements in the context of AML/CFT (ensuring that their private donors, suppliers, partners and intended beneficiaries are *bona fide* entities) and data protection laws (fulfilling data subjects' rights by providing minimum information on screening).

CONCLUSION

Larger international NGOs screen individuals to mitigate real or imagined risks in various contexts. This paper has hopefully contributed to earlier research on the international dimensions of data protection by conceptualising screening as a data processing operation and by considering NGOs' conduct with regards to providing information on screening to data subjects.

As screening is implemented by using personal data, it is a data processing operation. INGOs subscribing to screening technologies use basic personal information to run any search in the database and the search also yields a file containing further personal data (in case of positive and false positive hits). The results are used to identify and distinguish 'innocent' individuals from 'suspicious' ones – with whom the INGOs do not intend to interact with. Publicly available privacy notices, usually addressed to European (Western) audiences, almost never contain information on screening. As this information is missing, the principle of transparency (fairness, lawfulness) and data subjects' right to information are equally impacted, if not violated. Informal discussions with INGOs revealed that information on screening is provided orally to individuals, depending on the circumstances.

Reflecting on the limits of this paper, a pure legal analysis would have required access to internal NGO documents, policies and procedures to analyse facts (how NGOs themselves communicate with various categories of data subjects and how they document screening as a data processing activity) in light of the GDPR and related national legislation. As access, in the form of ethnographic research, for example, was not an option, the legal analysis could utilise only data collected by other social science methods. The gathered data were necessary to determine if screening is a data processing operation (it is), but data was not sufficient to analyse and conclude if NGOs comply with the transparency obligations of the GDPR. Any solid conclusion with regards to (non-)compliance with the transparency provisions of the GDPR would require the inclusion of specific laws in national jurisdictions (to see if they allow restrictions) and the domestic laws in aid recipient countries in the analysis. Therefore, INGOs need to consider the national legislation of the countries they are registered in to see if any exemption or restriction may apply with regards to the transparency obligation.

Transparency, however, is more than a legal principle. Beyond the narrow legal domain, the differential treatment of data subjects – depending on organisational perceptions of individuals' digital comprehension and the nature of the legal relationship between the individuals and the organisations – raises questions to be explored in the future.

NGOs, unlike banks, are organisations whose operations are dependant to a large extent on voluntarism. Their credibility depends on how they conform to the public image of solidarity and altruism. While screening may prevent fraud, the misuse of funds and ensure compliance with AML/CTF rules, inconsistent compliance with the transparency obligations of the GDPR might also undermine trust towards those delivering aid. If the reputation, credibility or legitimacy of an NGO is undermined – by screening or by screening in secret – not only the care and protection provided to local communities and individuals may be compromised, but the NGO may also lose their legitimacy, and as a result, donations too. Controversies around screening may entail unintended consequences on other human rights too – that may, in many cases, be better fulfilled by NGOs than by governments of aid recipient states controlling the given populations.

Beata Paragi is an Associate Professor at Corvinus University of Budapest, and has completed her Masters at University of Oslo on the topic of screening by NGOs in the context of aid work.

This paper is prepared with support from the Norwegian Centre for Humanitarian Studies Research Network on Humanitarian Efforts dynamic seed funding initiative, funded by the Research Council of Norway. The Legal Innovation Lab Oslo (University of Oslo) and Lovdata (Norway) also provided some funding for including the counter-terrorism perspective into the analysis.

The author wishes to thank her supervisor and the participants of the workshop that helped inform development of this paper. The responsibility is hers, feedback from colleagues or practitioners is most welcome (at beata.paragi@uni-corvinus.hu).

Suggested citation: Paragi, Beata. 2023. Opacity or transparency? Screening by NGOs in the context of aid work. NCHS Paper 10, April. Bergen: Norwegian Centre for Humanitarian Studies.

FOOTNOTES

[1] The academic literature (development studies) and law (in certain jurisdictions) distinguish NGOs working in the field of international development (NGDOs) from those organisations (charities, relief organisations) that are mostly active in the humanitarian field for humanitarian assistance to be provided free of donor concerns and interests, in line with the four humanitarian principles (neutrality, impartiality, humanity and indepedence). As the data protection requirements equally apply regardless to this categorisation, I would refer to them as INGOs (for the sake of simplicity) noting that when it comes to NGOs participation in counter-terrorism (CT) activities the difference may carry relevance. With regards to NGOs operating in the Global South, legal compliance equally includes laws in their country of origin (where the NGOs is established and based) and in the given location they operate (depending on the legal status of the NGO in the given aid recipient country).

[2] While screening is carried out by aid actors (NGOs) themselves, in case of vetting, NGOs are required to provide identity information of individuals and entities by the official donor (USAID, for example), which carries out the checks itself (Gillard, 2021a, 48). Wealth screening conducted by aid NGOs for fundraising purposes is a different matter, therefore, it is not considered in this paper (for its data protection dimension see Franz et al 2020).

[3] The paper is built on research conducted for the sake of an MA-thesis submitted to the University of Oslo in 2022the thesis itself conceptualised screening as a data processing operation and as a result, it addressed the matter of transparency both from legal and empirical perspectives. It is available upon request by email.

[4] Only one PN per NGO was publicly available with the exception of two organisations (NRC, PLAN UK). Larger NGOs may have multiple privacy notices (for internal use only) addressed to various groups of people (data subjects: candidates, employees, etc), which may be subject to change. For example, PLAN UK has revised the privacy notices since the data collection was closed (in November 2022); it used to have six PNs, in early 2023 there are now four. Three NGOs did not have a privacy notice. The full table is available at (by August 2023): PNs_NGOswebsites_22nov_without contacts.xlsx.

[5] *Screening as a data processing operation in aid work*. Workshop funded by NCHS, hosted by PRIO; Oslo, 23 September 2022. The primary purpose of the event was to provide an opportunity for practitioners to discuss the data protection dilemmas of screening, but participants were notified about my research and this NCHS-paper too.

[6] The essence of the GDPR is personal data protection, the purpose of which is to protect the fundamental rights of living, natural persons. Data is personal, following Article 4, if they relate to an identified or identifiable person, known as 'data subject.' Personal data may concern any information about a person whose identity is either clear or can be derived from additional information (EU Handbook, 2018, 83). Considering the international (non-European) impact of the GDPR, the regulation not only implies certain extraterritorial scope, but it is also ambitioned to serve as a normative instrument shaping privacy standards in global terms.

[7] Article 35 (data protection impact assessments) and Article 37 (the requirement for appointing a data protection officer) is not discussed in this paper.

[8] Annex II under *General conditions applicable to European Union-financed grant contracts for external actions* – Annex e3h2 (Article 1.5. bis), https://ec.europa.eu/trustfundforafrica/sites/default/files/annex_g_-_annex_ii_-_general_conditions_0.pdf.

[9] It should also be briefly mentioned that if a project is financed from the EU budget and the EU institutions are project owners, a sister-regulation governing data protection within the EU institutions also applies (EUDPR 2018).

[10] While secrecy in the context of national security and surveillance is to be distinquished from 'professional secrecy' conceptually, both can limit or restrict individuals' rights, even the transparency principle, (EU Handbook, 2018, 71) as long as such measures are in line with the legal conditions of restrictions. Professional secrecy is interpreted a 'special ethical duty that incurs a legal obligation inherent in certain professions and functions, which are based on faith and trust", for example, medical context, lawyer-client privilege, financial sector) (EU Handbook, 2018, 69).

[11] Recital 38 to Directive 95/46/EC; see also CJEU, *Smaranda Bara* C-201/14 (1 October 2015), para. 34, which says that "[i]t follows that the requirement of fair processing of personal data laid down in Article 6 of Directive 95/46 requires a public administrative body to inform the data subjects of the transfer of those data to another public administrative body for the purpose of their processing by the latter in its capacity as recipient of those data."

[12] As in the case of most German NGOs in the sample; the Jesuite Refugee Service (Italy) also has a very detailed 'web privacy notice': https://jrseurope.org/en/privacy-policy/. Others, for example, War Child Holland, claims that the privacy statement is addressed "for all individuals, companies and organisations involved in our work. This includes individual donors, large and small institutional donors, partner organisations implementing our work and *people who participate in our projects* or research … [with regards to those that have different kinds of relations to the NGO, separate PNs are used] our privacy statement does *not* address the processing of employee, intern, consultant or volunteer data, which is covered by other internal privacy documents and agreements https://www.warchildholland.org/yourprivacy/.

[13] See for example CARE NL: https://www.carenederland.org/privacy-statement.

[14] Interview with an advisor working at a Norwegian NGO, Teams, 4 May 2021.

[15] PRIO/NCHS workshop, Oslo, 23 September 2022.

LEGAL SOURCES

FATF (2015) *Best Practices Paper on Combating the Abuse of NonProfit Organisations. Recommendation 8.* https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html

EU GDPR (2016) *Regulation 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,* https://eur-lex.europa.eu/eli/reg/2016/679/oj

Article 29 WP (2007) *Opinion 4/2007 on the concept of personal data*. WP 136, 20. June 2007.

Article 29 WP (2018) *Guidelines on Transparency under Regulation 2016/679*, https://ec.europa.eu/newsroom/article29/items/622227

DCP (2021) *Whatsapp. Data Protection Commission, In the matter of the General Data Protection Regulation.* DPC Inquiry Reference: IN-18-12-2, 2021, https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf

EDPB (3/2018) *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*. Version 2.1., edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf (europa.eu).

EDPB (2/2019) *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Version 2.0*, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

EDPB (10/2020) *Guidelines 10/2020 on restrictions under Article 23 GDPR*, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_en.

EDPB (1/2022) *Guidelines 01/2022 on data subject rights – Right of access*. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en.

EU (2020) ANNEX II. *General conditions applicable to EU-financed grant contracts for external actions* (version: August 2020, 3h2_gencond_en); the practical guide on contract procedures for European Union external action (PRAG) is available at: https://ec.europa.eu/europeaid/prag/document.do?nodeNumber=1.

TFEU: *Treaty on the Functioning of the EU*, Article 288, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E288.

UNSC (2664/2022) S/RES/2664. *Adopted by the Security Council at its 9214th meeting, on 9 December 2022*, http://unscr.com/en/resolutions/doc/2664

ACADEMIC REFERENCES

Adams, R. (2020) *Transparency. New Trajectories in Law*. London, Routledge.

BADIL (2021) *European Union Conditional Funding: Its Illegality and Political Implications*. Badil Position Paper. Bethlehem: Badil, https://www.badil.org/cached_uploads/view/2021/04/20/europeanunionconditionalfunding-positionpaper-april2020-1618905422.pdf.

Becher, S. I. and Benoliel, U. (2020). Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR. In K. Mathis and A. Tor, eds, *Consumer Law and Economics*. Springer.

Bennett, Colin J (2018) The European General Data Protection Regulation: An instrument for the globalization of privacy standards? *Information Polity* 23 (2), 239-246.

Bygrave, L. A. (2014a) Core Principles of Data Privacy Law. *In Data Privacy Law: An International Perspective*. Oxford, online edn, Oxford Academic, https://doi.org/10.1093/acprof:oso/9780199675555.003.0005 (accessed 23 Sept. 2022).

Bygrave, L. A. and Luca Tosoni (2020) Article 4(1). Personal data. In Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary*. New York: Oxford Academic, online edn), https://doi.org/10.1093/oso/9780198826491.003.0007 (accessed 23 September 2022).

Charny, J. R. (2019) Counter-Terrorism and Humanitarian Action: The Perils of Zero Tolerance. Commentary. *War on the Rock*. https://warontherocks.com/2019/03/counter-terrorism-and-humanitarian-action-the-perils-of-zero-tolerance/.

Christensen, Z.; Nielsen, R.; Nielson, D. and Tierney, M. (2010) 'Transparency Squared: The effects of donor transparency on recipient corruption levels'. Paper prepared for application to participate in the 4th Annual Conference on the Political Economy of International Organizations for 2011, https://www.peio.me/wp-content/uploads/2014/04/Conf4_Christensen-Nielsen-Nielsen-Tierney-01.10.2010.pdf.

De Goede, M. (2018). The chain of security. *Review of International Studies*, 44(1), 24-42.

De Goede, M., G. Sullivan (2016) The politics of security lists. *Environment and Planning D: Society and Space* 34(1) 67–88.

de Terwangne, C. (2018) Principles (Articles 5–11) Article 5. Principles relating to processing of personal data. In Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Laura Drechsler (eds): *The EU General Data Protection Regulation (GDPR): A Commentary*. pp. 309-320.

Duffield, M. (2001) *Global governance and the new wars: the merging of development and security*. London: Zed.

Duffield, M. (2007) *Development, Security and Unending War: Governing the World of Peoples. London*: Polity Press.

Duffield, M. (2016) The resilience of the ruins: towards a critique of digital humanitarianism. *Resilience* 4(3): 147-165.

Eckert, S. (2022) Counterterrorism, sanctions and financial access challenges: Course corrections to safeguard humanitarian action. *International Review of the Red Cross*. No. 916-917 February 2022, https://international-review.icrc.org/articles/counterterrorism-sanctions-and-financial-access-challenges-916#footnote81_27rk033.

Federer, J. P. (2022) The Politics of Proscription and Peacemaking: Implications of Labelling Armed Groups as Terrorists and Extremists. *Journal of Intervention and Statebuilding*, DOI: 10.1080/17502977.2022.210736.

Franz, V., L. Hannah and B. Hayes (2020) *Civil Society Organizations and General Data Protection Regulation Compliance Challenges, Opportunities, and Best Practice*. Brussels: Open Society Foundation, available at: *civil-society-organizations-and-gdpr-compliance-20200210.pdf (reliefweb.int).

Gazi, T. (2020) Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. *Int J Humanitarian Action* 5 (9), https://doi.org/10.1186/s41018-020-00078-0.

Gillard, E. (2021a) *IHL and the humanitarian impact of counterterrorism measures and sanctions. Unintended ill effects of well-intended measures*. Chatham House Report, https://www.chathamhouse.org/2021/09/ihl-and-humanitarian-impact-counterterrorism-measures-and-sanctions/04-funding-agreements.

Gillard, E. (2021b) Screening of final beneficiaries – a red line in humanitarian operations. An emerging concern in development work. *International Review of the Red Cross* 103 (916-917): 517-537.

Gusterson, H. (2009) Ethnographic Research. In Klotz, A. and Prakash, D. (eds) *Qualitative Methods in International Relations*. New York, Palgrave.

Hayes, B. (2012) Counter-Terrorism, "Policy Laundering," and the FATF: Legalizing Surveillance, Regulating Civil Society. *The International Journal of Not-for-Profit Law* 12 (1-2), available at: https://www.icnl.org/resources/research/ijnl/1-introduction-2 or https://www.statewatch.org/media/documents/analyses/no-171-fafp-report.pdf.

Hayes, B. (2017) *The Impact of International Counter-Terrorism on Civil Society Organisations: Understanding the Role of the Financial Action Task Force*. Berlin: Bread for the World, http://efc.issuelab.org/resources/27481/27481.pdf.

Helgesson, K. S., & Mörth, U. (2019). Instruments of securitization and resisting subjects: For-profit professionals in the finance–security nexus. *Security Dialogue*, 50(3), 257–274.

HRC (2019) *Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders: report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, A/HRC/40/52. UN Human Rights Council.

Kaminski, M. (2019) *The Right to Explanation, Explained*, 34 Berkeley Tech Law Journal 189 (2019), available at https://scholar.law.colorado.edu/faculty-articles/1227.

Klareen, J. (2013) The Human Right to Information and Transparency. In Bianchi, A. and Peters, A. eds (2013) *Transparency in International Law*. Cambridge University Press, pp. 223-238.

Kuner, C. and Marelli, M., eds (2020) *Handbook on Data Protection in Humanitarian Action*. Second Edition, ICRC – Brussels Privacy Hub. https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

Minnella C.M. (2019). Counter-Terrorism Resolutions and Listing of Terrorists and Their Organizations by the United Nations. In: Shor E., Hoadley S. (eds) *International Human Rights and Counter-Terrorism*. International Human Rights. Springer, pp. 31-53.

NRC (2018a) Principles Under Pressure: the Impact Of Counterterrorism Measures And Preventing/Countering Violent Extremism On Principled Humanitarian Action. https://reliefweb.int/sites/reliefweb.int/files/resources/nrc-principles_under_pressure-report-screen.pdf.

NRC (2018b) Understanding Conditional Clauses. Oslo: Norwegian Refugee Council. Available at: https://www.nrc.no/shorthand/stories/understanding-counterterrorism-clauses/index.html and https://www.nrc.no/globalassets/pdf/reports/toolkit/nrc_toolkit_03_reviewing-counterterrorism-clauses.pdf.

Paragi, B. (2022) Challenges in Using Online Surveys for Research Involving Sensitive Topics: Data Protection Practices of European NGOs Operating in the Global South. *SAGE Research Methods Cases – Doing Research Online*, https://methods.sagepub.com/case/online-surveys-delicate-sensitive-topics-data-protection-european-ngos.

Paragi, B. (2022). The ambiguous politics of screening. *NCHS blog post*, https://www.humanitarianstudies.no/the-ambiguous-politics-of-screening/.

Polčák, R. (2018) Rights of the Data Subject (Articles 12–23) Section 1 Transparency and modalities Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject. In Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Laura Drechsler (eds): *The EU General Data Protection Regulation (GDPR): A Commentary*. pp. 397-412.

Schmidt, J. (2022) The European Union and the promotion of values in its external relations – the case of data protection. In J. Lee and A. Darbellay (eds) *Data governance in AI, FinTech and Legal Tech*. Cheltenham: Edward Elgar Tech, pp. 238-262.

Schudson, Michael (2018) *The Rise of the Right to Know. Politics and the Culture of Transparency*, 1945–1975. Harvard University Press.

Shabibi, N. and B. Bryant (2016) VICE News Reveals the Terrorism Blacklist Secretly Wielding Power Over the Lives of Millions. *VICE News*, 4 February 2016, available at: https://www.vice.com/en/article/pa4mgz/vice-news-reveals-the-terrorism-blacklist-secretly-wielding-power-over-the-lives-of-millions (accessed 20 January 2022).

Sullivan, (2020) *The Law of the List. UN Counterterrorism Sanctions and the Politics of Global Security Law*. Cambridge University Press.

Tosoni, L. and Lee A. Bygrave (2020) Article 4(2). Processing. In: Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds): *The EU General Data Protection Regulation (GDPR)*. Oxford University Press, pp. 116-123.

Tzanou, M. (2017) *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*. Oxford: Hart Publishing.

VOICE (2021) *Adding to The Evidence the Impacts of Sanctions and Restrictive Measures On Humanitarian Action*. Survey Report, March 2021, https://voiceeu.org/search?q=adding+to+the+evidence.

Vrabec, H. U. (2021) The Right to Information. In *Data Subject Rights under the GDPR* (Oxford, 2021; online edn, Oxford Academic, 22 July 2021).

Watson S, Burles R. (2018) Regulating NGO funding: securitizing the political. *International Relations*. 32(4):430-448.