Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR

Article *in* Journal of International Humanitarian Action · July 2020

DOI: 10.1186/s41018-020-00078-0

1 author:

Theodora Gazi
National and Kapodistrian University of Athens
4 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Gazi *Journal of International Humanitarian Action* (2020) 5:9
https://doi.org/10.1186/s41018-020-00078-0

Journal of International Humanitarian Action

REPORT Open Access

Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR

Theodora Gazi[1,2]

Abstract

Data collection is valuable before, during and after interventions in order to increase the effectiveness of humanitarian projects. Although the General Data Protection Regulation (GDPR) sets forth rules for the processing of personal data, its implementation by humanitarian aid actors is crucial and presents challenges. Failure to comply triggers severe risks for both data subjects and the reputation of the actor. This article provides insights into the implementation of the guiding principles of the GDPR, the legal bases for data processing, data subjects' rights and data sharing during the provision of humanitarian assistance.

Keywords: GDPR, Personal data, Humanitarian assistance, NGOs

Introduction: defining data protection during humanitarian assistance

The collection of personal data is crucial for the provision of humanitarian assistance; it allows humanitarian aid actors to identify those in need and deliver aid, where necessary. Processing of personal data occurs throughout the response cycle to increase situational awareness, conduct evaluations, support ongoing operations and secure the delivery of assistance. The wide range of humanitarian needs, including food, housing, health services, legal aid, interpretation and education, results in the continuous processing of beneficiaries' information. Typically, this data is stored in both paper copies and digital form, and it consists of records of services received, family details, photographs and health data.

Apart from the operational value of collecting data, this information may provide unique humanitarian aid actors with insight into the context, beneficiaries' needs and the type of assistance required. Moreover, data analysis may support risk assessments and facilitate the identification of vulnerable cases, based on previously identified patterns and personal characteristics. For instance, the Humanitarian Data Exchange platform of the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) has been utilising data, since 2018 to inform decision-making on displacement in South Sudan, the Ebola outbreak in the Democratic Republic of Congo and cash assistance in Somalia (OCHA, 2019). This was also the case in Bangladesh, where floods regularly impact vulnerable population; OCHA collaborated with the International Organization for Migration (IOM) and identified refugee camps at risk of flooding, based on satellite images, drone footage and other sources (Telford, 2020).

While access to data is crucial, poor information management may spark violence and discrimination in situations of persecution. Specifically, groups of persons might be targeted, even when they are not directly identifiable, e.g. following the publication of a report or a situation analysis. Moreover, failure to protect data confidentiality may lead to stigma and ultimately threaten the actors' reputation, putting both employees and beneficiaries at risk.

Correspondence: thgazi@hotmail.com
[1]Faculty of Law, National and Kapodistrian University of Athens, Athens, Greece
[2]Danish Refugee Council (DRC Greece), Athens, Greece

Due to these sever risks, it is essential that humanitarian aid actors, such as international organisations (IOs), non-governmental organisations (NGOs), charities and volunteer groups, respect the fundamental principles of data protection and adopt relevant policies, when providing humanitarian assistance around the globe. For decades, aid actors established in the European Union (EU) have been implementing emergency response and development projects in third countries. Meanwhile, millions of migrants have crossed into Europe since 2015, sparking the refugee crisis and the continuous processing of data by aid actors. The existing literature on the application of the General Data Protection Regulation (GDPR) during humanitarian assistance is limited, despite the fact that its implementation presents unique challenges, i.e. large-scale data processing, language barriers and the vulnerability of the data subjects. To enrich our understanding about these issues, this article focuses on the implementation of the GDPR by aid actors established in the EU.

It should be noted that based on guidelines from the European Data Protection Board (EDPB, 2019), the application of the GDPR to IOs is without prejudice to international law provisions and must be viewed in light of any privileges and immunities that an IO enjoys (Kuner, 2020). For this purpose, IOs which enjoy immunities, such as UNHCR (UNHCR, 2015) and IOM (IOM, 2010), have adopted and published internal data protection policies/strategies to promote the respect of human dignity and the well-being of data subjects during humanitarian interventions within or outside the EU.

GDPR key definitions and guiding principles

The right to privacy and to control the use of personal information is recognised as a fundamental right in the EU. The General Data Protection Regulation (GDPR)[1] came into force in May 2018, serving as a comprehensive legislation on data processing by the public and private sector, directly applicable across EU member states. On the one hand, the GDPR applies to humanitarian aid actors established in the European Union (EU) which process personal data[2]. Whether data subjects are in or outside the EU is irrelevant, since the GDPR does not solely protect EU nationals, when the organisation is EU-based. On the other hand, the GDPR is applicable to actors established outside the EU, where they offer services to beneficiaries located within the EU, irrespective of whether payment is required[3].

The key definitions for data protection, i.e. for "personal data", "processing" and "special categories of data", are provided in articles 4 and 9. *Personal data* is any information relating to a living natural person, who can be identified directly or indirectly through said information, i.e. a name, an identification number, location data and other factors specific to his/her identity. Different pieces of information, which may lead to the identification of a particular person when combined also constitute personal data. Furthermore, any operation performed on personal data, including its collection, storage, alteration, retrieval, use, dissemination and erasure is regarded as *processing* of data. Finally, *special categories of data* (*sensitive data*) revealing ethnic origin, political, philosophical and religious beliefs, trade union membership, health, genetic and biometric data, in addition to sex life and sexual orientation, are considered sensitive, due to the fact that its processing may create significant risks for a person's fundamental rights and freedoms.

Each actor must incorporate the guiding principles of data processing prior to data collection, based on article 5 of the GDPR. First, actors need to identify a valid legal basis for processing personal data (*lawfulness* principle). Emphasis must be given to the principles of *fairness* and *transparency*; at the time of data collection, individuals must not be misled and they should always be aware of the identity of the actor who is collecting their information, the purpose of processing and their data rights. The GDPR emphasises that the requirement to provide this information using clear and plain language is of particular importance when addressing vulnerable individuals and children. However, the provision of information to beneficiaries in their own language by the actors' cultural mediators or in writing is particularly challenging, especially in the EU context where persons from multiple countries of origin reside in the same refugee camp.

Furthermore, based on the principle of *purpose limitation*, the actor must firstly identify the personal data to be processed and the processing purpose, while designing the intervention ("data by design"). This data may not be reused for other incompatible purposes. For instance, legal aid provision requires the processing of beneficiaries' data, including special categories of data. The actor may publish a press release containing

[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) [2016] OJ L119/1.

[2]"This 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" (article 3 paragraph 1 of the GDPR).

[3]"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union" (article 3 paragraph 2 of the GDPR).

personal stories based on data acquired while providing legal aid if and only if it has the subjects' explicit consent.

Additionally, actors should only process information which is essential for service provision (principles *of data minimisation* and *proportionality*). For instance, the distribution of catered food in a refugee camp requires the processing of the beneficiaries' full name and documentation so as to verify their residential status. Based on data minimisation, processing of other categories of data, such as marital status or country of origin, is not necessary for conducting said distribution. However, special circumstances may justify the processing of additional data. If cultural mediators are needed to facilitate the distribution, the beneficiaries' country of origin or ethnicity would be necessary to determine the interpreting language or regional dialect. In reality, the implementation of data minimisation and proportionality is challenging, when personal data is collected to demonstrate accountability towards donors. Specifically, there is always the risk, if not the certainty in certain response environments, of collecting unnecessary personal data for the sake of producing donor reports (Behnam & Crabtree, 2019). While these reports are aggregated and contain anonymised data, thus confidentiality is maintained, aid workers might "run in circles" to collect additional information and end up losing sight of their core mission to provide assistance and solely process necessary data.

In addition, beneficiaries' data must be processed accurately (*accuracy principle*). For example, it is necessary to regularly update the organisation's beneficiary record, to ensure that individual cases are traced and followed-up throughout the year.

Moreover, although archiving personal data might be tempting, it must not be kept indefinitely (*storage* limitation). In certain cases, the retention period is determined based on the relevant national legislation or the organisation's legitimate interests, e.g. donors' audit requirements to retain documentation for a fixed time period after the conclusion of the project. Either way, organisations should set retention periods, after which the data will be erased or anonymised.

While information security is sometimes overlooked when designing an intervention, it is a key requirement for humanitarian organisations. Poor information security may cause severe harm to beneficiaries, considering the sensitive categories of data processed by organisations. This means that technical and organisational measures must be adopted to ensure that data can be accessed exclusively by authorised personnel and that it remains accessible and recoverable, in case of accidental loss (principles of *integrity and confidentiality*).

The GDPR recognises pseudonymisation and anonymisation as appropriate technical measures for enhanced security of data processing, because they reduce the impact of data breaches and support actors in complying with data protection principles. The two techniques differ substantially and the choice between them depends on the nature of the data and the risks associated with data processing. In particular, the GDPR introduces the process of pseudonymisation as a new concept in European data protection law for rendering data neither anonymous nor directly identifiable. Pseudonymisation, i.e. replacing names or other direct identifiers with codes and/or numbers, is a de-identification process, referenced as both a security and a data protection "by design" mechanism to safeguard personal data (articles 25 paragraph 1, 32 paragraph 1 and 89 of the GDPR). This way, data may no longer be attributed to a specific individual, without the use of additional information, provided that said information is kept separately (article 4 case 5 of the GDPR). Pseudonymisation could go beyond the concealment of real identities by supporting "unlinkability" (Esayas, 2005) and contributing towards data minimisation, when access to real identities is not needed (e.g. electronic file of cases handled to produce quantitative reports). While pseudonymous data is not exempted from the scope of the GDPR, it serves as a security measure, facilitating the storage of sensitive data and information sharing with partners.

In contrast, anonymisation is a procedure where data is rendered anonymous and the data subject is not identifiable; thus, the information may be processed without applying data protection provisions (recital 26 of the GPDR). Once data are anonymised, all identifying information is eliminated and subjects are no longer identifiable. In cases where data is successfully anonymised, the GDPR provisions cease to apply. Humanitarian organisations routinely attempt to anonymise personal data. However, it is often difficult to determine whether data has been sufficiently anonymised, since individuals may be re-identified, by combining other datasets or contextual understanding, especially when the group of data subjects is not sufficiently large.

Legal bases for data processing during humanitarian aid

Conditions for processing personal data

Based on article 6 of the GDPR, the relevant legal bases, for processing personal data during a humanitarian intervention, are (a) consent of data subject, (b) contractual obligation, (c) legitimate interests and (d) protection of the beneficiaries' or another person's vital interests. Moreover, recital 46 suggests that vital interests may apply, when processing data on humanitarian grounds, such as to monitor epidemics, or where there is a

natural or man-made disaster causing a humanitarian emergency.

Although the need of the NGO to record humanitarian needs and displacement patterns is evident, there is not a "one size fits all" legal basis for data collection. In reality, determining the legal grounds for processing information is not straightforward.

First, while consent is considered one of the most common bases for processing, in many cases, it could be invalid during humanitarian interventions. Consent must be freely given, specific, informed and unambiguous (article 7 and recital 32 of the GDPR). It should be a real choice of the data subject, who may freely revoke his/her consent at any point. However, when providing vital assistance to people in need, the concept of consent might be non-existent. Consent is not freely given—thus not valid—when a person's access to essential services depends on the processing of their data. Under this scope, NGOs must refrain from using this legal basis when collecting data from vulnerable people to provide assistance. Moreover, when data is collected based on consent, assessing a person's vulnerability involves understanding the social and cultural norms, so that the choice is not made for the population. In any case, it is imperative that goods and services are not withheld, even if individuals are not willing to consent to the processing of their information.

Second, the organisation may rely on vital interest as legal basis, when data processing is necessary to protect someone's life, health, dignity and security. Due to the emergency situations in which organisations usually operate, processing of data may be based on vital interest, when offering assistance (such as distribution of food, water, mattresses and medical assistance). It should be noted that beneficiaries must always be provided with sufficient information regarding data processing and be given the opportunity to object, as soon as possible, ideally during data collection, e.g. through posters or handouts in their native language.

Third, fulfilment of a contractual obligation could also be used as a legal basis to process data. In this context, the term "*contract*" should not be interpreted as a formal document to which the data subject is party (ICO, 2019), but as an agreement between the organisation and the beneficiaries to offer and receive services without valuable consideration. Broadly speaking, this means that the organisation may process personal data, where it is necessary in order to offer said services or in order to take steps at the request of the beneficiaries, prior to providing a service needed.

Finally, humanitarian organisations may process personal data when it is necessary for their "legitimate interests". This could apply when data is collected for the effective performance of the mission or for accountability purposes as required by donors. In these situations, processing data must be necessary, rather than convenient, provided that it has a minimal privacy impact and the organisation's legitimate interest is not overridden by the fundamental rights and freedoms of the data subjects.

Conditions for processing sensitive data

Humanitarian actors engaged in protection or assistance activities, such as legal aid and health services may need to process sensitive data. Processing special categories of data is prohibited in principle, except for limited circumstances described in article 9. While ten legal bases are established and extensively described in the GDPR, the most relevant for processing sensitive data in the humanitarian context are summarised and presented below:

(a) Explicit consent of the data subject for one or more specified purposes
(b) Vital interests of the data subject or of another person when physically or legally incapable of giving consent
(c) Not-for-profit bodies when processing beneficiaries' data in connection with their purposes
(d) Data manifestly made public by individuals
(e) Establishment, exercise or defence of legal claims
(f) Reasons of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care
(g) Preventive or occupational medicine, medical diagnosis and provision of health care or treatment
(h) Research and statistic purposes, e.g. patient registries for improving diagnoses and therapies.

Actors should only process sensitive data when absolutely required for the fulfilment of their mission and in line with their mandate. Most importantly, relying on the appropriate basis does not release the actor from the responsibility to assess the risk of processing beneficiaries' data.

Data protection impact assessments

In case an activity is likely to pose a high risk for individuals, a data protection impact assessment (DPIA) must be carried out prior to data collection, based on article 35. A DPIA contains a description of the envisaged activity, policy or data transfer involving the processing of personal data, a risk analysis of the rights of data subjects, the categories of personal data processed, in addition to the safeguards and measures taken to ensure the protection of the data.

Assessing the level of risk requires examining both the likelihood and the severity of the potential harm. The

outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that data processing complies with the GDPR. Where a DPIA indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures, a consultation with the supervisory data protection authority should be initiated prior to the processing.

For instance, a DPIA would be appropriate in the following scenarios:

a. UNHCR requests access to the list of all residents in a refugee camp on a monthly basis maintained by the CCCM (Camp Coordination and Camp Management) actor, in order to examine their eligibility for cash assistance. The DPIA would examine the necessity of sharing, risks of regular data transfers to an IO, the categories of data to be shared and other potential risks to data rights.
b. Due to continuous break-ins of the actor's office inside the refugee camp, its management decides to dispose of hard copies of supporting documentation and upload soft copies in a web-based storage platform. In this scenario, the DPIA would explore the categories of data processed, whether said platform provides adequate safety measures, any potential risks to data rights, and access control procedures, in addition to information integrity and availability of the data uploaded.

DPIAs are crucial during project design in order to safeguard compliance with data protection provisions. They are tailored to each particular intervention; subsequently, they differ between organisations and projects. DPIAs enable the identification of privacy risks for individuals, the development of risk mitigation strategies, as well as the protection of the actors' reputation. Useful DPIA templates and guidance have been developed by the International Committee of the Red Cross (ICRC, 2017) and the French supervisory data protection authority (CNIL, 2018).

Sharing data with other aid actors

The effectiveness of a humanitarian response relies on compiling data lists, e.g. of camp residents, communities in need and other potential beneficiaries. In situations of emergency, aid actors are often asked to share this data with other organisations to support the humanitarian intervention. This exchange of information is crucial, in order to avoid repeated data collections from the same data subjects and overlap of services offered.

At the point of considering sharing data with third parties, an assessment must be conducted on whether the sharing is within the original lawful basis for processing and whether data subjects were made aware of the circumstances of a prospective sharing. In all cases, appropriate safeguards must be used, such as contractual clauses binding the recipient to provide appropriate data protection. Data sharing agreements are typically established when organisations regularly exchange data to provide humanitarian assistance. These agreements specify the roles and responsibilities of the parties involved, stipulate additional restrictions or protective measures on how the data is used and indicate the categories of data and the transfer modalities. It should be noted that different types of data transfer agreements may be needed, depending on the categories of data, the applicability of national laws and the actors involved. More specifically, special attention is required when sharing data with IOs, which constitute their own "jurisdiction" and data flows are regulated based on cross-border transfers to third countries, even when their mission is within the EU.

Data rights

When receiving humanitarian assistance, beneficiaries must be able to understand and exercise their rights. The GDPR provides the following rights for individuals:

a. *The right to be informed* (articles 13 and 14). The transparency principle compels actors to inform their beneficiaries in writing or orally regarding data processing, in a manner and language that is understandable to them. Exercising this right in the humanitarian context presents many challenges, e.g. actors need to produce written privacy notices, have them translated and shared in multiple languages; mass arrivals trigger emergency responses which hinder information sharing; and in cases of illiteracy, alternative methods need to be explored, such as info sessions with trained cultural mediators.
b. *The right to access* (article 15). Upon request, the beneficiary may receive confirmation as to whether his/her data is being processed, as well as information on the data processed. Recital 63 of the GDPR specifies that the right to receive a copy of the data shall not adversely affect other people's rights and intellectual property. Moreover, the actor may ask the data subject to specify the type of information or processing activities their request relates to.
c. *The right to rectification and erasure* (articles 16 and 17). The beneficiary may request the correction or deletion of personal data, which is inaccurate, unnecessary or excessive.
d. *The right to restrict processing and object* (articles 18 and 21). When the processing is based on the

legitimate interests of the actor (in cases of data processing for donor accountability or reporting purposes as mentioned above), the beneficiary has the right to object, on grounds relating to his/her particular situation. He/she may request the restriction of processing, when the accuracy of data is contested or the processing is either unlawful or unnecessary.

e. *The right to data portability* (article 20). The beneficiary has the right to receive his/her personal data, in a structured, commonly used and readable format, and request the direct transmission of data to other actors, when data processing is based on contractual obligations and made by automated means. In reality, direct data transmission via standardised interagency forms is a common practice between actors operating in Europe, so as to refer beneficiaries upon their request to services of specialised providers, e.g. medical appointment or counselling sessions.

In addition, data subjects must be informed without undue delay, in other words as soon as possible, about data breaches, when it is likely to result in a high risk to their rights and freedoms (article 34). Assessing said "high risk" is linked to the severity of the potential or actual impact on individuals, due to the breach. The greater the likelihood of the consequences, the higher the risk. The rationale of this obligation is to allow individuals to adopt measures to mitigate the risk and protect themselves from the consequences of a security breach. In the refugee context, a breach that results in an accidental disclosure of beneficiaries' records to unauthorised third parties is likely to significantly impact affected individuals. Therefore, subjects would need to be informed about the breach. However, the accidental deletion of beneficiaries' records, which may be electronically restored, is unlikely to result in a high risk, so individuals in this case would not be informed about the breach.

Enabling beneficiaries to exercise their rights is a demanding task for aid actors. It requires successfully tracking all processing activities, recording requests and responding timely to all requests received, within 1 month from reception, which may be extended to 2 additional months from reception in case of numerous or complex requests (article 12 paragraph 3).

The role of the Data Protection Officer

The Data Protection Officer (DPO) role is an important innovation and a cornerstone of the GDPR's accountability-based compliance framework. DPOs are persons with expert knowledge of data protection law and practices. They need to be able to perform their duties and tasks in an independent manner, whether or not they are employed by the actor. The appointment of a DPO is mandatory for actors when their core activities involve large-scale processing that requires regular and systematic monitoring of data subjects or large-scale processing of special categories of personal data. While the GDPR does not define large-scale processing, the factors to be taken into consideration include the number of individuals concerned, either as a specific number or as a proportion of the relevant population; the volume of data being processed; and the duration and the geographical extent of the data processing activity (Article 29 Data Protection Working Party, 2017). Based on these criteria, the majority of aid actors fall under the obligation to appoint a DPO, since their core activities involve large-scale processing of information and sensitive data.

In the humanitarian context, the DPO must be familiar with data protection and security requirements, as well as the actor's standard operating procedures (SoPs), policies and codes of conducts. The main tasks of a DPO include monitoring compliance with the GDPR and national legislation, informing and advising management on data protection mainstreaming and training staff. Moreover, the DPO provides advice during data protection impact assessments, monitors their performance and acts as a contact point for beneficiaries and the supervisory data protection authority on issues related to the processing of data.

Conclusion

Data protection is a longstanding priority during humanitarian assistance. It could be conceived as an aspect of the *"do no harm"* principle, which requires humanitarian actors to endeavour not to cause further damage and suffering as a result of their actions. Indeed, during humanitarian interventions, data can serve as a tool to accelerate development, combat poverty and contribute to informed decision-making.

Aid actors established in the EU which process beneficiaries' personal data residing within or outside Europe must both apply the GDPR and efficiently deliver aid services. While the use of new technologies may notably facilitate data collection, experimentation in the humanitarian setting is not acceptable without a clear ethical approach. A risk-based approach needs to be adopted prior to data collection ("privacy by design") and new processing techniques must only be implemented following a data protection impact assessment.

Moreover, beneficiaries of humanitarian aid are not consumers; thus, data protection must never disrupt the provision of humanitarian assistance. At the same time, processing vulnerable people's data is a heavy duty compared to collecting data for business transactions or

marketing purposes. The specificities of the humanitarian sector demand data responsibility, even for non-personal data, i.e. the adoption of enhanced measures and precautions when collecting sensitive information which do not constitute personal data by law. For example, the locations of safe houses and medical facilities in conflict settings can expose residents and patients to risk and must be treated as sensitive, even if this information is not considered to be personal data by law. The same applies for survey results and datasets containing information that could be used to target individuals in a conflict area.

Finally, data protection and humanitarian assistance should be viewed as complementary fields, since their purpose is to safeguard human rights and fundamental freedoms of data subjects. Balancing between competing rights (e.g. between data protection and freedom of expression or the right to liberty and security) is made *ad hoc*, in accordance with the principle of proportionality and with the objective to protect human dignity.

Abbreviations

DPIA: Data protection impact assessment; DPO: Data protection officer; EU: European Union; GDPR: General Data Protection Regulation; IO: International organisation; IOM: International organisation for migration; NGO: Non-governmental organisation; OCHA: United Nations Office for the Coordination of Humanitarian Affairs

Acknowledgements

NA

Author's contributions

The author read and approved the final manuscript.

Authors' information

The conclusions presented in the article stem from the author's daily work and implementation of the relevant legislation during humanitarian aid projects.

Funding

No funding was received for the research.

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Competing interests

The author declares that she has no competing interests.

Received: 7 January 2020 Accepted: 8 July 2020
Published online: 16 July 2020

References

Article 29 Data Protection Working Party (2017) Guidelines on Data Protection Officers. http://ec.europa.eu/newsroom/document.cfm?doc_id=44100. Accessed 3 Mar 2020

Behnam N, Crabtree K (2019) Big data, little ethics: confidentiality and consent. Forced Migration Review (61). https://www.fmreview.org/sites/fmr/files/FMRdownloads/en/ethics/ethics.pdf . Accessed 3 Mar 2020

CNIL (2018) Privacy impact Assessment (PIA) Template. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf. Accessed 3 Mar 2020

EDPB (2019) Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf. Accessed 3 Mar 2020

Esayas SY (2005) The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach. European Journal of Law and Technology, 6 (2)

ICO (2019) Guide to the General Data Protection Regulation (GDPR). https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Accessed 3 Mar 2020

ICRC (2017) Handbook on data protection in humanitarian action (Kuner, C. & Marelli, M., Eds.)

IOM (2010) IOM data protection manual. https://publications.iom.int/system/files/pdf/iomdataprotection_web.pdf. Accessed 3 Mar 2020

Kuner C (2020) The GDPR and international organizations. AJIL Unbound 114:15–19. https://doi.org/10.1017/aju.2019.78

OCHA (2019) Annual report 2018. https://www.unocha.org/sites/unocha/files/OCHA2018AnnualReport.pdf. Accessed 3 Mar 2020

Telford S (2020) Opinion: In a world awash with data, aid workers contend with gaps. https://news.trust.org/item/20200205170710-56ry0. Accessed 3 Mar 2020

UNHCR (2015) Personal data of persons of concern to UNHCR. https://www.refworld.org/pdfid/55643c1d4.pdf. Accessed 3 Mar 2020

Publisher's Note