

# DATA PROTECTION STANDARDS FOR HUMANITARIAN ORGANIZATIONS AND PARTNERS

## OBJECTIVES

- Equip participants with a clear understanding of the core principles of data protection, especially in the humanitarian sector and African context.
- Explore the specific challenges of implementing data protection in humanitarian contexts within Africa and identify practical solutions for overcoming these challenges.
- Encourages consideration of the ethical, legal, and operational aspects of data protection in a humanitarian setting, taking into account the fragmented data protection arena.
- Highlight the best practices, principles and strategies for data sharing with donors and third parties, ensuring compliance with both local and international standards.

## INTRODUCTION

Humanitarian response increasingly relies on digital means as a result of advancement in technologies and efforts to make humanitarian action more efficient and to better reach affected populations. With the increase of the interweaving of societies and rise of technology, the issue of data has become an important matter – both its uptake and its protection, noting the importance of taking different contexts/ regions/ cultures into consideration. With this advancement, data protection legislation is rapidly evolving, and now more than 100 countries have data protection laws, and new ones continue to be drafted as awareness of the need to protect data spreads throughout the world.

Africa has emerged as the fastest-growing digital environment characterized by a rapid proliferation of digital technological innovations, mobile phone adoption, and e-commerce platforms. At the same time, the continent also grapples with many crises as a result of armed conflict and other situations of violence, natural disasters inter alia, where many humanitarian actors operate. With this comes the need to obtain data which may drive the efficiency of humanitarian action. Therefore, the need arises as to how such data is protected for the benefit of affected people; maintain credibility and transparency, strengthen relations with stakeholders; and provide a basis for governance change. While African countries have made effort to enact legal frameworks of data protection, key challenges arise. This session takes us into the intricacies of what data protection in humanitarian action entails; the African context of data protection; and most importantly – the basic principles data sharing generally and specifically with donors and third parties.

## OVERVIEW OF DATA PROTECTION IN HUMANITARIAN ACTION

In an increasing world of new technologies, and need to make processes efficient, fast and providing interconnectedness globally, has seen the increase of processing a wide – array quantities of data. In the humanitarian context globally, data is crucial for the provision of humanitarian assistance<sup>1</sup> which in most cases, involves processing of

<sup>1</sup>Gazi, T. Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. Int J Humanitarian Action 5, 9 (2020). <https://doi.org/10.1186/s41018-020-00078-0>; <https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00078-0>

personal and sensitive data. Humanitarian organizations handle vast amounts of data from affected people, donors, and partners. Therefore, it is key to have robust protection measures in place that not only protect the affected persons but create an accountable and conducive environment for donors and third-party partners.

Globally there are tools that have been developed. These international instruments dealing with data protection set important benchmarks for humanitarian organizations operating globally and in Africa. These include:

1. General Data Protection Regulation (GDPR)<sup>2</sup> – European Union: The GDPR is one of the most comprehensive data protection laws globally and has set a high standard for personal data protection. Although it primarily applies to EU countries, the GDPR affects organizations globally, including those in Africa, if they process the data of EU citizens or collaborate with European partners.<sup>3</sup>
2. The OECD Privacy Framework (2013)<sup>4</sup>
3. the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)<sup>5</sup> including Protocol CETS No. 223 amending the Convention (now known as Convention 108+)<sup>6</sup>
4. UN General Assembly Resolution 45/95 of 14 December 1990<sup>7</sup> adopting the Guidelines for the Regulation of Computerized Personal Data Files<sup>8</sup> which includes the humanitarian clause calling for particular care and flexibility when applying data protection principles in the humanitarian sector<sup>9</sup>
5. the UN Principles on Personal Data Protection and Privacy, adopted by the UN High-Level Committee on Management (HLCM) at its 36th Session on 11 October 2018<sup>10</sup>.
6. the International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution) adopted by the ICDPPC in Madrid in 2009<sup>11</sup>
7. African Union Convention on Cyber Security and Personal Data Protection adopted in June 27, 2014<sup>12</sup>

International humanitarian organizations have also developed critical tools for data protection as they work across different jurisdictions. These include

1. the ICRC Rules on Personal Data Protection<sup>13</sup>

<sup>2</sup> General Data Protection Regulation (GDPR): <https://gdprinfo.eu/>

<sup>3</sup> GDPR Local, *GDPR & Data Protection Laws in Africa: A Comparison*, Posted on November 29, 2023, available at <https://gdprlocal.com/gdpr-and-data-protection-laws-in-africa-a-comparison/#:~:text=GDPR%20has%20an%20extraterritorial%20reach,jurisdictions%20but%20not%20beyond%20it.>

<sup>4</sup> OECD Privacy Guidelines, available at <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>

<sup>5</sup> CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 28 January 1981, in force 1 October 1985, ETS 108: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108>

<sup>6</sup> CoE, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 10 October 2018, CETS 223: <https://rm.coe.int/16808ac918>

<sup>7</sup> UN General Assembly Resolution 45/95 of 14 December 1990, A/RES/45/95 14 December 1990

<sup>8</sup> UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990: <http://www.refworld.org/docid/3ddcafaac.html>.

<sup>9</sup> ICRC handbook, Handbook on Data Protection in Humanitarian Action – Second Edition

ref. 4305.01, available at <https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action-pdf-en.html>

<sup>10</sup> UN High-Level Committee on Management (HLCM), UN Principles on Personal Data Protection and Privacy, 18 December 2018: <https://unsceb.org/principles-personal-data-protection-and-privacy-listing>

<sup>11</sup> International Conference on Data Protection and Privacy Commissioners, International Standards on the Protection of Personal Data and Privacy: [https://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf?mc\\_phishing\\_protection\\_id=28047-br1tehqu81eaoar3q10](https://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf?mc_phishing_protection_id=28047-br1tehqu81eaoar3q10)

<sup>12</sup> [African Union Convention on Cyber Security and Personal Data Protection | African Union \(au.int\)](https://au.int/en/press/20140627-african-union-convention-on-cyber-security-and-personal-data-protection)

<sup>13</sup> Aimed at safeguarding individuals' personal data, particularly in challenging situations such as armed conflicts and other humanitarian emergencies. ICRC Rules on Data Protection: <https://shop.icrc.org/icrc-rules-on-personal-data-protection-print-en.html>

2. the ICRC Professional Standards for Protection Work<sup>14</sup>
3. UN Personal Data Protection and Privacy Principles<sup>15</sup>
4. UNHCR Data Protection Policy (formally known as the Policy on the Protection of Personal Data of Persons of Concern)<sup>16</sup> As well as the UNHCR General Policy on Personal Data Protection and Privacy<sup>17</sup>
5. UNICEF Policy on Personal Data Protection<sup>18</sup>

## AFRICAN CONTEXT

As noted above, data is crucial in humanitarian contexts. The African continent has several crises mandating humanitarian intervention including in situations of armed conflict and other situations of violence, natural disasters among others. This makes strong data protection measures essential for maintaining trust and ensuring that humanitarian aid is delivered ethically and safely.

The legal regime on data protection within Africa is quite fragmented. Certain regional instruments have tried to provide a foundation but are marred by inadequacies. The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)<sup>19</sup>, which was adopted in 2014 may be seen as the first African continent-wide legal instrument addressing personal data protection and cybersecurity. As mentioned by *Data Protection Legal Regime and Data Governance in Africa: An Overview* Policy Brief the Convention seeks to ‘*harmonize the laws of member states on data protection and encourage member states to create frameworks to protect personal data within the continent.*’<sup>20</sup> In Additional to the Convention, the African Union Commission (AUC) and the Internet Society (ISOC), jointly developed the “[Personal Data Protection Guidelines for Africa](#)”, which is a detailed set of best practice guidelines on personal data protection.

The Southern African Development Community (SADC) Model Law on data protection<sup>21</sup> developed for ICT, can be application to humanitarian contexts in some extent. One critique made about the SADC Model Law on Data protection was that ‘*although it provided a compulsory requirement for data transfer to only take place between SADC members or non-members with adequate data mechanisms, it does not provide the parameters for determination of such level of adequacy.*’<sup>22</sup> The Economic Community of West African States (ECOWAS) region has the [ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection \(2010\)](#) while the East African Community has a draft document on EAC Legal Framework for Cyber Laws that was published in November 2008.<sup>23</sup>

<sup>14</sup> ICRC, *Professional Standards for Protection Work*: <https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights>

<sup>15</sup> [UN Principles on Personal Data Protection & Privacy. FINAL \(1\) \(1\) \(unsceb.org\)](#)

<sup>16</sup> UNHCR Data Protection Policy: [https://help.unhcr.org/turkiye/wp-content/uploads/sites/11/2018/12/DataProtectionPolicy\\_ENG.pdf](https://help.unhcr.org/turkiye/wp-content/uploads/sites/11/2018/12/DataProtectionPolicy_ENG.pdf)

<sup>17</sup> [General Policy on Personal Data Protection and Privacy | Refworld](#)

<sup>18</sup> [UNICEF Policy on Personal Data Protection](#)

<sup>19</sup> Malabo Convention: [https://au.int/sites/default/files/treaties/29560-treaty-0048\\_-\\_african\\_union\\_convention\\_on\\_cyber\\_security\\_and\\_personal\\_data\\_protection\\_e.pdf](https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf)

<sup>20</sup> Olumide Babalola, *Data Protection Legal Regime and Data Governance in Africa: An Overview* Policy Brief, February 2022 African Economic Research Consortium (AERC Africa): <https://aercafrica.org/old-website/wp-content/uploads/2022/02/DG003.pdf>

<sup>21</sup> Southern African Development Community (SADC) Model Law on data protection:

<sup>22</sup> Olumide Babalola, *Data Protection Legal Regime and Data Governance in Africa: An Overview* Policy Brief, February 2022 African Economic Research Consortium (AERC Africa): <https://aercafrica.org/old-website/wp-content/uploads/2022/02/DG003.pdf>

<sup>23</sup> <http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?seq> accessed on 17 November 2020.

Some of the African countries have developed their own model laws that apply within their borders. As of January 2024, 36 out of 55 African countries (65%) now have a data protection law'.<sup>24</sup> Since then, the list has been expanded with data protection law in Malawi and Ethiopia. The pace for enactment of laws has increased especially in the last decade. ALT notes that traditionally Francophone countries, 75% have adopted a data protection law; for Southern African countries 73% now have a law in place and 54% of countries in East Africa have enacted laws.<sup>25</sup>

As noted before, humanitarian action requires data, and while some countries in Africa have taken the necessary steps to provide protection, there are a couple of challenges. These include the inadequate regulatory frameworks; complexity of data flows and systems involved with partners, donors and affected people; conflict and instability that makes data security challenging; inadequate digital infrastructure that may increase data breaches; inadequate capacity in data protection methods. For example, the East African countries that have specific legislation has been criticized that they fail to meet internationally accepted standards like, for example, not having clear and independent authorities to oversee and manage personal data and privacy<sup>26</sup>.

## PRINCIPLES OF DATA PROTECTION

The above instruments provide a foundation especially principles which are taken into account in data protection. Such principles, though they may vary in application across different jurisdictions, serve to provide a framework of how data is collected, collated and shared in a manner uphold holds fundamental rights; adhere to laws, and policies; ethical considerations; and assist in effective humanitarian operations.

The principle of lawfulness, fairness and transparency touches on establishing a valid legal basis for processing data; and ensuring fairness and transparency processing data. The limitation purpose principles serve to require that humanitarian organizations show the specific, explicit and legitimate purposes for processing data in humanitarian context. The principle of proportionality espouses on the consideration of actions be appropriate to be pursued. This principle is closely tied to the data minimization principle which denotes that only the necessary data needed for the humanitarian operation should be collected<sup>27</sup>. The principle of accuracy requires that data must be accurate and up-to-date as this form part of credibility. The principle of integrity and confidentiality ensures that it is securely stored and protected from unauthorized access, accidental loss, or damage. This there requires 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.*”<sup>28</sup> The principle of storage limitation ensures that data is stored for a particular period of time – no longer than the specified, explicit and legitimate purposes.

<sup>24</sup> Data Protection ALT, *Mapping the progress (and delays) for data protection in Africa*: <https://dataprotection.africa/data-protection-in-africa-progress/#:~:text=As%20of%20January%202024%2C%2036,in%20enacting%20data%20protection%20legislati on.>

<sup>25</sup> Data Protection ALT, *Mapping the progress (and delays) for data protection in Africa*: <https://dataprotection.africa/data-protection-in-africa-progress/#:~:text=As%20of%20January%202024%2C%2036,in%20enacting%20data%20protection%20legislati on.>

<sup>26</sup> CIPESA, *Robust Data Protection Standards Could Spur Regional Economic Integration*: <https://cipesa.org/2024/03/robust-data-protection-standards-could-spur-regional-economic-integration/>

<sup>27</sup> ICRC handbook, *Handbook on Data Protection in Humanitarian Action – Second Edition*

ref. 4305.01, available at <https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action-pdf-en.html>

<sup>28</sup> Gazi, T. Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. *Int J Humanitarian Action* 5, 9 (2020). <https://doi.org/10.1186/s41018-020-00078-0>; <https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00078-0>

## GUIDING QUESTIONS

- What are the key data protection principles applicable in Africa, that humanitarian organizations should prioritize when collecting and processing personal data?
- How can humanitarian organizations balance the urgent need for collecting and sharing personal data to deliver aid effectively, while ensuring compliance in the context of Africa's diverse legal and technological landscape?
- To ensure privacy and security of humanitarian action data while balancing the need for accountability to donors, what are the best practices for sharing data with donors?
- How can humanitarian organizations ensure that third-party service providers comply with data protection standards, especially when their primary focus is profit?
- What are the main challenges that humanitarian organizations face in protecting personal data in Africa?
- How can humanitarian organizations build stronger regulatory and operational safeguards to overcome challenges associated with data protection in these contexts?

## ADDITIONAL MATERIAL

- ICRC handbook, Handbook on Data Protection in Humanitarian Action – Second Edition ref. 4305.01 , available at <https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action-pdf-en.html>
- ICRC Rules on Data Protection: <https://shop.icrc.org/icrc-rules-on-personal-data-protection-print-en.html>
- ICRC, *Professional Standards for Protection Work*: <https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights>
- Olumide Babalola, *Data Protection Legal Regime and Data Governance in Africa: An Overview* Policy Brief, February 2022 African Economic Research Consortium (AERC Africa): <https://aercafrica.org/old-website/wp-content/uploads/2022/02/DG003.pdf>
- Data Protection ALT, in its *Mapping the progress (and delays) for data protection in Africa*: <https://dataprotection.africa/data-protection-in-africa-progress/#:~:text=As%20of%20January%202024%2C%2036,in%20enacting%20data%20protection%20legislation.>
- Gazi, T. Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. *Int J Humanitarian Action* 5, 9 (2020). <https://doi.org/10.1186/s41018-020-00078-0>; <https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00078-0>
- ODPC Handbook <https://www.odpc.go.ke/wp-content/uploads/2024/02/PERSONAL-DATA-PROTECTION-HANDBOOK.pdf>
- Personal Data Protection Guidelines for Africa – A joint initiative of the Internet Society and the Commission of the African Union, 9 May 2018: [https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines\\_2018508\\_EN.pdf](https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf)