sciendo

International Organizations and AI-Supported Humanitarian Aid: Navigating through the Applicable (Data Protection) Legal Regimes

Maruša T. Veber

University of Ljubljana, Slovenia
marusa.veber@pf.uni-lj.si

VEBER, T. Maruša. International Organizations and AI-Supported Humanitarian Aid: Navigating through the Applicable (Data Protection) Legal Regimes. *International and Comparative Law Review*, 2024, vol. 24, no. 2, pp. 54–83. DOI: 10.2478/iclr-2024-0018

Summary: The increasing reliance of international humanitarian organisations on artificial intelligence (AI) to fulfil their mandates gives rise to a number of legal issues, including those pertaining to data protection and the role of individual consent. By focusing on the law and practice of the World Food Programme (WFP) this paper makes a twofold contribution. First, it argues that the enforcement of relevant national and regional data protection and AI legal regimes in relation to the work of international humanitarian organizations is generally precluded by the immunities to which they are entitled under international law. It is therefore the internal regimes of these organisations that provide the most relevant legal framework governing the use of AI and subsequent data gathering. Second, this paper demonstrates that, rather than focusing on the notion of consent, humanitarian organisations should prioritise the incorporation of robust safeguards for data protection and the responsible use of AI into their respective internal regimes.

Keywords: humanitarian assistance, artificial intelligence, international organizations, data protection, immunities, consent, GDPR, AI Act

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

1 Introduction

The delivery of humanitarian aid is becoming increasingly reliant on artificial intelligence (AI).[1] AI systems[2], which typically draw on large amounts of data, including biometric data of beneficiaries, significantly improve the accuracy and effectiveness of aid delivery.[3] By distributing aid with the help of AI, international humanitarian organizations (humanitarian IOs) aim to ensure that their assistance reaches those in need, thereby preventing the aid from being diverted and used for other purposes. On the other hand, the use of AI in this humanitarian context gives rise to a plethora of legal issues, including those pertaining to data protection and the role of consent from affected individuals.[4] This is particularly pertinent given the growing capacity of AI systems to link "data or recognising patterns

---

1 This paper was prepared in the framework of a research project 'Development and use of artificial intelligence in light of the negative and positive obligations of the state to guarantee the right to life (J5–3107)', which is co-funded by the Slovenian Research Agency (ARIS). It is partially based on a shorter contribution in a post conference publication T. VEBER, Maruša. AI-Supported Humanitarian Aid and the Right to Life: Highlighting Some of the Legal Challenges Faced by International Humanitarian Organizations. In: SANCIN, Vasilka (ed.). *Artificial Intelligence and Human Rights: From the Right to Life to Myriad of Diverse Human Rights Implications*. Ljubljana, Litteralis 2025 (forthcoming). See also T. VEBER, Maruša. Artificial Intelligence and Humanitarian Assistance: Reassessing the Role of State Consent. *Ljubljana Law Review*, 2024, vol. 84, pp. 217–253.

2 There is currently no uniform definition of the AI. Arguably the most authoritative definition was provided in the UNESCO Recommendation, whereby AI systems are understood as "systems which have the capacity to process data and information in a way that resembles intelligent behaviour, and typically includes aspects of reasoning, learning, perception, prediction, planning or control." UNESCO Recommendation on the Ethics of Artificial Intelligence. [online]. Available at <https://unesdoc.unesco.org/ark:/48223/pf0000380455>. Accessed: 1.2024, para. 2. It is acknowledged, however, that the definition of AI will have to be changed over time following the rapid technological developments.

3 BEDUSCHI, Ana. Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks. *International Review of the Red Cross,* 2022, vol. 104, issue 919, pp. 1149–1169; KAYHAN, Halid. Using Biometrics to Provide Humanitarian Aid… While the 'data hunt' to identify "security threats" is on the rise?! (PART I). [online]. Available at: <https://www.law.kuleuven.be/citip/blog/using-biometrics-to-provide-humanitarian-aid-part-i/>. Accessed: 7.8.2024.

4 NARBEL, Vincent Graf, SUKAITIS, Justinas. Biometrics in humanitarian action: a delicate balance. *Humanitarian Law & Policy*, 2021. [online]. Available at: <https://blogs.icrc.org/law-and-policy/2021/09/02/biometrics-humanitarian-delicate-balance/>. Accessed: 20.4.2023; EUROPEAN DATA PROTECTION BOARD. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 2022. [online]. Available at: <https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf >. Accessed: 20.4.2023, p. 10; FRA. Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2020. Available at: <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf>. Accessed: 7.8.2024; KUNER, Christoper, MARELLI, Massimo. *Handbook on Data Protection in Humanitarian Action. Second edition*. ICRC, 2020. [online]. Available at: <https://www.icrc.org/en/data-protection-humanitarian-action-handbook>. Accessed: 5.5.2024, pp. 280–296; PIRVAN, Petruta. EU GDPR applicability to international organizations. iapp, 2021. [online]. Available at: <https://iapp.org/news/a/eu-gdpr-applicability-to-international-organizations/>. Accessed: 7. 8. 2024.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

of data [which] may render non-personal data identifiable."[5] These issues are particularly salient in the context of humanitarian IOs, given the lack of clarity in international law regarding the extent to which these organisations are bound by relevant international, regional and national data protection and AI legal regimes.

By focusing on the law and practice of the World Food Programme (WFP), one of the leading organisations responsible for the delivery of humanitarian aid in the context of both man-made and natural disasters, this paper makes a twofold contribution. First, it outlines the ways in which different data protection and AI legal regimes apply to IOs. Even though regional regimes (e.g. that of the European Union (EU)) seem to extend some of its data protection and AI provisions (extraterritorially) to humanitarian IOs, it is argued here that the enforcement of these regimes is precluded in relation to humanitarian IOs, regardless of whether their activities would fall within the territorial and material scope of these regimes. Against this background, it is the internal, institutional data protection and AI regimes of humanitarian IOs, that primarily govern their activities when delivering aid with the support of AI.

Second, this paper delineates the internal data protection and AI policies of the United Nations (UN), with a particular focus on the WFP. It highlights that WFP's data protection regime is centred on the notion of individual consent, but at the same time questions the appropriateness of such an approach in a humanitarian context where it is often difficult to establish informed and freely given consent. It is therefore suggested that, rather than focusing on the notion of consent, arguably the broadest and all-encompassing legal basis for gathering and processing data, WFP and, humanitarian organizations generally, should work on incorporating sufficient safeguards for data protection and safe use of AI into their respective internal regimes, thereby protecting beneficiaries and their human rights when interacting with these organizations.

A few caveats have to be put forward before we discuss these issues further. First, this paper only focuses on the delivery of aid by IOs, such as the UN special agencies, and not non-governmental organizations (NGOs) mandated with the delivery of aid. As NGOs are not subjects of international law properly so-called, they are primarily governed by national laws, while the application of international legal rules applies differently to them than to IOs.[6] Second, it is acknowledged, that humanitarian action is governed by international legal rules other than

---

5 CENTRE FOR INFORMATION POLICY LEADERSHIP. Artificial Intelligence and Data Protection in Tension, First Report, 2018. [online]. Available at: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf>. Accessed: 7.8.2024, p. 10; BARBOZA, Julia Zomignani, JASMONTAITĖ-ZANIEWICZ, Lina, DIVER, Laurence. Aid and AI: The Challenge of Reconciling Humanitarian Principles and Data Protection. *14th IFIP International Summer School on Privacy and Identity Management (Privacy and Identity)*. 2019, Windisch, Switzerland, pp. 161–170.

6 KUNER, MARELLI (n 4), p. 81. Generally on non-governmental organizations see: LINDBLOM, Anna-Karin. *Non-Governmental Organisations in International Law*. Cambridge: Cambridge University Press 2009.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

those analysed in the paper, including the general humanitarian assistance legal regime, based on the guiding principles of humanitarian assistance,[7] international humanitarian law and the general international human rights law.[8] However, this paper leaves aside the discussions arising from these rules as it only focuses on the analysis and the application of international, regional and institutional data protection and AI regimes to humanitarian IOs. It also has to be acknowledged that it is not the aim of this paper to present in detail the content of the international and regional regimes on data protection and AI. Rather, the aim is to discuss their application to humanitarian IOs. Third, AI systems may be used by humanitarian IOs not only for improving the delivery of aid but also to make predictions to detect natural and manmade disasters, identify the needs of affected populations, as well as automated mapping of disaster areas and outbreaks of pandemics that may occur in the context of humanitarian crises.[9] These other uses of AI in humanitarian action and legal issues arising from them are, however, not addressed in this paper, which focuses on humanitarian aid delivery and the use of AI. Finally, it is acknowledged that, beyond data security, there exist other concerns and risks which are increasingly put forward when discussing various AI solutions, such as arbitrary decision-making, difficulties in establishing responsibility, transparency challenges, difficulties in assuring the accuracy and reliability of AI systems, as well as propagation of bias and possible discriminative effects of the use of AI.[10] These are especially pertinent in humanitarian contexts involving vulnerable individuals.[11] However, analyzing these issues falls beyond the ambit of this contribution.

Following this introduction, this paper briefly presents the practice of the use of AI by humanitarian IOs, with specific focus on WFP (section 2). It then outlines the international and, regional, in particular, EU data protection and AI legal regimes, which specifically refer to humanitarian IOs and their work (section 3). More importantly, it explains that, regardless of the (extra)territorial and material scope of the relevant regional legal regimes, their enforcement against humanitarian IOs is precluded on account of the immunities that IOs are entitled to under general international law (section 4). Subsequently, the paper analyses internal IOs provisions on data protection and AI, focusing specifically on the

---

7 For example, the use of AI by humanitarian IOs may be in contradiction with the right to privacy and the fundamental humanitarian principles embedded in the work of humanitarian IOs such as humanity, impartiality, and no harm principle. UNGA Resolution 46/182, 19. December 1991, UN Doc. 46/182; BARBOZA, JASMONTAITĖ-ZANIEWICZ, DIVER (n 5), p. 162.

8 More on this see T. VEBER 2024 (n 1).

9 BARBOZA, JASMONTAITĖ-ZANIEWICZ, DIVER (n 5), p. 164.

10 For example, in Sweden, thousands of unemployed people were denied benefits by a government systems that used AI. EUROPEAN DATA PROTECTION BOARD (n 4), p. 10; Further on this see: KUNER, MARELLI (n 4), pp. 285–286, 296.

11 BAKER, Fran, ETYEMEZIAN, Hovig, MORENO JIMÉNEZ, Rebeca. AI for efficient, evidence-informed humanitarianism. UNHCR Innovation Service, 2024. [online]. Available at: <https://medium.com/unhcr-innovation-service/ai-for-efficient-evidence-informed-humanitarianism-fd246238a0ad>. Accessed: 7.8.2024.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

WFP and the role of individual consent (section 5). Finally, the paper offers some concluding remarks (section 6).

2 The Use of AI in Humanitarian Aid Delivery

Humanitarian IOs are increasingly using AI to fulfil their humanitarian mandates. According to the WFP, the use of AI has several benefits:

> Well-managed data, supported by effective knowledge management, and advances in analytics, Artificial Intelligence and Machine Learning, can cut the time it takes to deliver life-saving aid and empower our teams to design smarter and more effective ways of working.[12]

Indeed, the benefits of using AI in humanitarian aid delivery are many and include optimising responses, reducing response times, improving the accuracy and effectiveness of aid delivery, helping to prevent potential misuse of humanitarian aid, and individualising humanitarian aid.[13] Against this background, WFP committed itself to "becoming a digitally enabled and data-driven organization, with investments in new technology"[14] and introduced different AI solutions into its activities. For example, in partnership with the United Nations High Commissioner for Refugees (UNHCR), an iris scan payment system has been implemented in a refugee camp in Jordan, allowing 76,000 Syrian refugees to purchase food from camp supermarkets using a scan of their eye instead of cash, vouchers or e-cards.[15] This system allows communication with different databases within seconds (e.g. the UNHCR and bank databases) with the aim of fast and efficient aid delivery. By tying the distribution of aid to the use of AI and biometrics, the WFP aims to ensure that aid gets into the hands of those in need and to prevent it from being diverted and used for other purposes.[16] However, on the other hand, such use of AI opens manifold important legal questions.

In particular, the use of AI systems in humanitarian assistance may be problematic from the point of view of increasing profiling of individuals combined with the possible dual use of the collected data by these systems and from the point of view of data security. This is the case because the operation of the AI

12 WFP Global Data Strategy 2024–2026. [online]. Available at: <https://reliefweb.int/report/world/wfp-global-data-strategy-2024–2026>. Accessed: 7.8.2024.

13 SLIM, Hugo. Eye Scan Therefore I am: The Individualization of Humanitarian Aid. European University Institute, 2015. [online]. Available at: <https://iow.eui.eu/2015/03/15/eye-scan-therefore-i-am-the-individualization-of-humanitarian-aid/>. Accessed 7.8.2024. See also T. VEBER 2024 (n 1), pp. 218–221.

14 WFP strategic plan (2022–2023). WFP/EB.2/2021/4-A/1/Rev.2, 12 November 2021, para. 130.

15 WFP Introduces Iris Scan Technology To Provide Food Assistance To Syrian Refugees In Zaatari. WFP, 2016. [online]. Available at: < https://reliefweb.int/report/jordan/wfp-introduces-iris-scan-technology-provide-food-assistance-syrian-refugees-zaatari>. Accessed: 20.8.2024.

16 UN food chief warns aid suspension in Yemen likely to start this week. Reuters, 2019. Available at: <https://www.reuters.com/article/us-yemen-security-un/u-n-food-chief-warns-aid-suspension-in-yemen-likely-to-start-this-week-idUSKCN1TI1X7>. Accessed: 20.8.2024.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

systems is based on the collection of a large amount of data, including personal data enabling the identification of a concrete individual.[17] These systems typically don't gather only 'soft biometrics' such as height, age, gender, and eye colour but also 'hard biometrics' traits like iris scans or vein patterns, capable of identifying specific individuals through reverse engineering.[18] Similarly, facial recognition does not merely identify a person but also reveals a lot of information about a person (e.g. their ethnicity, age range, etc.).[19] This is problematic as such data can easily be used for other purposes and turned into tools of surveillance, security checks, tracing or deportation.[20] In the past, states have requested access to biometric data of refugees from humanitarian IOs for use in security checks and deportation procedures.[21] Possible involuntarily disclosure of personal data of, for example, refugees or asylum seekers, may endanger the lives of these individuals if retrieved by their countries of origin.[22] Moreover, the WFP was accused of poor data handling[23] and there were cases whereby cyber-attacks on the systems of humanitarian organizations exposed the personal data of about 500,000 vulnerable people across the world.[24]

What is more, humanitarian IOs increasingly rely on private commercial actors to support their humanitarian activities. Eloquent is an example of the WFP which recently partnered with Palantir, to use their software to provide faster and more efficient food assistance to those in need.[25] Palantir is a leading US company specializing in data analytics, which is also increasingly integrating AI in various aspects of its operation and is ranked among the top AI software platforms.[26]

---

17 NARBEL, SUKAITIS (n 4).

18 KUNER, MARELLI (n 4), p. 93.

19 NARBEL, SUKAITIS (n 4).

20 MARTIN, Aaron, SHARMA, Gargi, DE SOUZA, Siddarth Peter, TAYLOR, Linnet, VAN EERD, Boudewijn, MCDONALD, Sean Martin, MARELLI, Massimo, CHEESMAN, Margie, SCHEEL, Stephan, DIJSTELBLOEM, Huub. Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions. *Geopolitics,* 2023, vol. 28, No. 3, pp. 1363–1397.

21 In the past Bangladesh, Lebanon, Malaysia and the US for example requested access to UNHCR biometric data on refugees. Ibid., p. 1382.

22 KUNER, Christopher. International Organizations and the EU General Data Protection Regulation: Exploring the Interaction between EU Law and International Law. *International Organizations Law Review*, 2019, vol. 16, no. 1, p. 160.

23 PARKER, Ben. Audit exposes UN food agency's poor data-handling. The New Humanitarian, 2018. [online]. Available at: <https://www.thenewhumanitarian.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling>. Accessed: 7.8.2024.

24 MACDONALD, Ayang. African nations must implement safeguards against humanitarian digital ID risks: researcher. Biometric update, 2022. [online]. Available at: <https://www.biometricupdate.com/202209/african-nations-must-implement-safeguards-against-humanitarian-digital-id-risks-researcher>. Accessed: 20.4.2024.

25 PARKER, Ben. New UN deal with data mining firm Palantir raises protection concerns. The New Humanitarian, 2019. [online]. Available at: <https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp>. Accessed: 20.4.2024.

26 Palantir Ranked No. 1 in Worldwide Artificial Intelligence Software Study in Market Share and Revenue. Businesswire, 2022. [online]. Available at: <https://www.businesswire.com/news/home/20220920006178/en/Palantir-Ranked-No.-1-in-Worldwide-Artificial-Intelligence-Software-Study-in-Market-Share-and-Revenue>. Accessed: 20.8.2024.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

However, in the past Palantir was subject to criticism due to allegations of supplying controversial data-sifting software to US government agencies.[27] In this respect the term 'surveillance humanitarianism' is sometimes used to describe the possible widespread collection of data in a humanitarian context and without appropriate safeguards, which may "inadvertently amplify the vulnerability of individuals in need of humanitarian aid;"[28] or even 'techno-colonialism' whereby practices of digital innovation "can lead to reproducing the colonial relationships of dependency and inequality amongst different populations around the world."[29]

All of these issues raise the question of the applicability of different data protection and AI regimes that would protect individuals when interacting with humanitarian IOs. For example, it is questionable whether the use of AI systems is compatible with existing data protection legal frameworks requiring *inter alia* appropriate legal basis for the processing of personal data, such as freely given and informed consent.[30]

3 Legal Regimes governing the Use of AI systems

3.1 International Legal Regimes

Individuals affected by man-made or natural disasters are entitled to the protection and respect of their human rights in accordance with international law,[31] including data protection. By way of a preliminary remark, it has to be acknowledged that provisions of AI-supported humanitarian aid open manifold human rights-related questions, however, the focus of this paper is solely on the application of data protection and AI legal regimes to the work of IOs, thereby leaving aside the questions relating to for example, more generally, the right to privacy.[32]

---

27 BARBOZA, JASMONTAITĖ-ZANIEWICZ, DIVER (n 5), p. 162; MARTIN, SHARMA, DE SOUZA, TAYLOR, VAN EERD, MCDONALD, MARELLI, CHEESMAN, SCHEEL, DIJSTELBLOEM (n 20), p. 1363.

28 LATONERO, Mark. Stop Surveillance Humanitarianism. New York Times, 2019. [online]. Available at: <https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html>. Accessed: 10.8.2024; BEDUSCHI (n 3), p. 1152.

29 MADIANOU, Mirca. Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises. Social Media & Society, 2019, Vol. 5, No. 3; BEDUSCHI (n 3), p. 1152. See also T. VEBER 2024 (n 1), pp. 220–221.

30 TIEDRICH, Lee, CAIRA, Celine, BENHAMOU, Yaniv. The AI data challenge: How do we protect privacy and other fundamental rights in an AI-driven world?. OECD AI Policy Observatory, 2023. [online]. Available at: <https://oecd.ai/en/wonk/the-ai-data-challenge-how-do-we-protect-privacy-and-other-fundamental-rights-in-an-ai-driven-world>. Accessed: 7.8.2024.

31 Article 5, ILC, Draft Articles on the Protection of Persons in the Event of Disasters. Yearbook of the International Law Commission, 2016, vol. II, Part Two.

32 As opposed to the right to privacy, which is firmly embedded in the international human rights framework and national legislation, data protection has only recently acquired the status of a fundamental right. It is generally recognised that data protection and privacy are inherently connected, constituting, however, two "distinctive but overlapping rights." While indeed data protection originates from the right to privacy, the relationship between the two has been subject to debate and is still controversial in some respects. However, it is beyond the confines of this paper

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

General human rights treaties such as the Universal Declaration of Human Rights[33] and the International Covenant on Civil and political Rights[34], do not include specific provisions on data protection and AI, and are in this sense, technologically-neutral. The most notable international legal framework concerning data protection is the Council of Europe's (CoE) 1981 Convention for the protection of individuals with regard to automatic processing of personal data,[35] which provides for common minimal standards concerning data protection at the international level.[36] Convention was supplemented with the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[37] and revised with the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+)[38] in 2018. The latter currently has 55 parties, including non-members of the CoE and is open to signature to IOs[39]. However, currently, no IO is a party to this convention. Under Convention 108+, data processing is based on the "free, specific, informed and unambiguous consent

---

to further dwell on this relationship, which solely focuses on data protection regimes. More on this see: DIGGELMANN, Oliver, CLEIS, Maria Nicole. How the Right to Privacy Became a Human Right. *Human Rights Law Review*, 2014, Vol. 14, Issue 3, pp. 441–458; HILDEBRANDT, Mireille. *Law for Computer Scientists and Other Folk*. Oxford: Oxford University Press, 2020, pp. 130–131; FORDE, Aidan. The Conceptual Relationship between Privacy and Data Protection. *Cambridge Law Review*, 2016, Issue 1, pp. 135 – 149; BRKAN, Maja. The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. German Law Journal, 2019, Vol. 20, Special Issue 6, pp. 864–883. For the right to privacy see also: Article 12, UN General Assembly, Universal Declaration of Human Rights, 217 A (III), 10 December 1948; Article 17 UN General Assembly, International Covenant on Civil and Political Rights, UNTS, vol. 999, p. 171, 16 December 1966; General Comment 16, Human Rights Committee (1988); Article 8, Council of Europe, European Convention on Human Rights, as amended by Protocols Nos. 11, 14 and 15, ETS No. 005, 4 November 1950; Article 7 Charter of Fundamental Rights of the European Union, *OJ C 326, 26.10.2012, p. 391–407*; Article 11, Organization of American States (OAS), American Convention on Human Rights, „Pact of San Jose", Costa Rica, 1969; Articles 16 and 21, League of Arab States, Arab Charter on Human Rights, 1994; Article 16, Convention on the Rights of the Child, United Nations, Treaty Series, vol. 1577, p. 3, 1989, Article 14, International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families, A/RES/45/158, 18 December 1990, and Article 22, Convention on the Rights of Persons with Disabilities: UN General Assembly Resolution, A/RES/61/106, 2007.

33 UNGA, Universal Declaration of Human Rights, 217 A (III), 10 December 1948.

34 UNGA, International Covenant on Civil and Political Rights, UNTS, vol. 999, p. 171, 16 December 1966.

35 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108.

36 Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe Treaty Series No. 223), 2018.

37 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No 181 (2001).

38 Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, opened for signature on 10 October 2018, CETS No 223.

39 Art. 27(1), Convention 108+.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

of the data subject" or other legitimate basis laid down by law.[40] The Convention also includes provisions on the adoption of appropriate security measures for the protection of personal data,[41] transparency of processing[42] and safeguards for the data subject such as the right to obtain rectification or erasure of data.[43] It also limits transboundary flows of personal data[44] and includes provisions on supervisory authorities.[45] In relation to the former, Article 14(2) of the Convention 108+ explicitly mentions IOs and stipulates:

> When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured.

Therefore, provisions on data protection from Convention 108+ may have (albeit informal) implications for data protection standards of IOs not parties to this convention, as it may serve as a form of conditionality. As will be explained below, a similar provision in included in the EU data protection and AI legal regimes.

CoE recently also adopted the first international treaty regulating the development and use of AI systems, which stresses the need for the application of the existing human rights obligations to the development and use of AI systems, and provides some concrete safeguards in this respect. The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Framework Convention on AI)[46] is based on the following fundamental principles: human dignity and individual autonomy, equality and non-discrimination, respect for privacy and personal data protection, transparency and oversight, accountability and responsibility and reliability and safe innovation. Article 4 of the Convention serves a as general human rights protection safeguard:

> Each Party shall adopt or maintain measures to ensure that the activities within the lifecycle of artificial intelligence systems are consistent with obligations to protect human rights, as enshrined in applicable international law and in its domestic law.

Furthermore, Article 11 stipulates that measures have to be taken to make sure that in the course of the activities within the lifecycle of AI personal data are protected, including through applicable domestic and international laws,

---

40 Art. 5, Convention 108+.
41 Art. 7, Convention 108+.
42 Art. 8, Convention 108+.
43 Art. 9, Convention 108+.
44 Art. 11, Convention 108+.
45 Chapter IV, Convention 108+.
46 Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series – No. [225] (2024).

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

standards and frameworks.[47] It also establishes a risk and management framework, whereby "measures for the identification, assessment, prevention and mitigation of risks posed by artificial intelligence systems by considering actual and potential impacts to human rights, democracy and the rule of law" are to be adopted by state parties.[48] The Framework Convention is open for signature to states and EU since September 2024.

These CoE conventions provide an important legal framework concerning data protection and AI, however, they are of limited relevance to humanitarian IOs which are not parties to these Conventions and are unlikely to become one in the future (with the possible exception of the EU). While IOs can take into account relevant provisions of CoE Conventions, they are not legally bound to do so. Alternatively, humanitarian IOs could potentially be bound by data protection and AI-related obligations through customary international law, once it is recognized that it has developed in these areas.[49]

3.2 Regional Legal Regimes

Arguably, the most comprehensive data protection regime evolved at the EU level. The EU Data Protection Directive,[50] the EU General Data Protection Regulation (GDPR)[51] and the newly adopted Data Act[52] address the issue of data gathering, whereas the AI Act specifically governs the use of AI. Additionally, data gathering and data analysis are also regulated by the EU human rights framework, whereby the Charter of Fundamental Rights of the European Union includes a

47 Art. 11, Framework Convention on AI.

48 Art. 16, Framework Convention on AI

49 It is acknowledged that some aspects of the right to privacy are considered as being part of customary international law, however, this arguably does not include (fragmented) standards on data protection as codified in the Convention 108+ and GDPR. See e.g. WATT, Eliza. *State Sponsored Cyber Surveillance, The Right to Privacy of Communications and International Law*. Edward Elgar Publishing, 2021; KITTICHAISAREE, Kriangsak, KUNER, Christopher. The Growing Importance of Data Protection in Public International Law. EJIL:Talk!, 2015. [online]. Available at: <https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/>. Accessed: 7.8.2024. For the view that data privacy has crystallized into a customary international law see ZALNIERIUTE, Monika. An international constitutional moment for data privacy in the times of mass-surveillance. *International Journal of Law and Information Technology*, 2015, Vol. 23, Issue 2, pp. 99–133.

50 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (no longer in force).

51 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) (GDPR).

52 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

specific provision on the protection of personal data,[53] which may be limited only under specific circumstances.[54] At the forefront of EU data regulation are "safeguards so that the persons whose data have been processed have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access or use of that data."[55] Against this background, the cornerstone EU data protection regime, GDPR, operates on the basis of the following main principles: lawfulness of processing (appropriate legal basis),[56] fairness of processing,[57] transparency of processing,[58] purpose limitation,[59] data minimisation,[60] data accuracy,[61] storage limitation,[62] data security,[63] and accountability.[64]

At the heart of EU data processing rules, including in the humanitarian context, is the need to have an adequate legal basis for processing personal data, which is primarily derived from the consent of the data subjects.[65] However, in the emergency situations, in which humanitarian IOs typically operate, obtaining valid, informed and freely given consent is often difficult. Moreover, in situations of humanitarian distress, when people are vulnerable and in need, a lack of alternatives (e.g. there is no possibility of receiving aid without the use of AI and data gathering), may contribute to the impossibility of receiving a valid consent.[66] Sometimes it is even impossible to obtain consent because of security concerns, logistical issues and the scale of the humanitarian operation. In such cases, where consent cannot be validly obtained, personal data may still be collected and processed on two alternative legal grounds: the vital interests of the data subject and reasons of public interest.[67] This means that if it is established that it is in the

53 Art. 8, Charter of Fundamental Rights of the EU. See also Arts 1 (human dignity) and 7 (respect for private life). Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391–407.

54 Art. 52(1) Charter of Fundamental Rights of the EU.

55 CJEU, Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, para. 54.

56 Arts 5(1)(a) and 6 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, GDPR).

57 Art. 5(1)(a) GDPR.

58 Ibid.

59 Art. 5 (l)(b) GDPR.

60 Art. 5(1)(c) GDPR.

61 Art. 5 (l)(d) GDPR.

62 Art. 5(1)(e) GDPR.

63 Art. 5 (1)(f) GDPR.

64 The data controller is responsible for, and must be able to demonstrate compliance with, the personal data processing principles contained in the GDPR. Art. 5(2) GDPR.

65 Art. 6 GDPR.

66 KUNER, MARELLI (n 4), p. 61.

67 GDPR, para 12 for example allows for the transfer of personal data to an international humanitarian organisation, "with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts,

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

vital interest of the data subject to process his or her data in order to protect "an interest which is essential for the Data Subject's life, integrity, health, dignity, or security or that of another person"[68] his or her personal data may be processed in the absence of the consent. This includes the provision of essential needs for individuals in humanitarian emergencies.[69]

More importantly, under the 'reasons of public interest' exception, personal data may be processed, when the concerned humanitarian activity is part of the mandate of a concerned entity under international law. As explained in the GDPR:

> 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.[70]

The GDPR therefore explicitly refers to humanitarian activities. To the extent that the processing of personal data is necessary to carry out their humanitarian tasks, under the GDPR humanitarian IOs could do so without the consent of the individuals concerned, as the valid legal basis would be the public interest or the vital interest of the data subject. The GDPR therefore contains data protection provisions and safeguards relevant to the work of humanitarian IOs, but under what conditions are they considered to be bound by these provisions?

The territorial scope of GDPR is determined under Article 3(1) as "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." An IO with an office or representation in the EU would therefore be considered to have an EU establishment.[71] Further, under Article 3(2), the GDPR may also apply to processing carried out by data controllers and data processors without an EU establishment when the processing activities are related to "the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union" or to "the monitoring of their behaviour as far as their behaviour takes place within the Union."[72] However, as the majority of WFP's activities take place outside the territorial scope of the GDPR, the impact of these provisions on the work of WFP and humanitarian IOs in general appears to be low.

---

could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject." KUNER (n 22).

68 KUNER, MARELLI (n 4), p. 66.

69 Ibid., pp. 66–67.

70 Recital 46, GDPR.

71 GDPR, recital 22 states that "establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."

72 For a detailed account see KUNER (n 22), p. 173.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

It is another aspect of GDPR that sparked the most attention from IOs, including the UN and its agencies. GDPR specifically refers to data transfers to humanitarian IOs:

> Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.[73]

This seems to allude that data transfers to humanitarian IOs are to be governed by the GDPR. GDPR also explicitly requires data controllers to provide information about their dealings with IOs, and gives access rights to individuals concerning such information. Under Articles 13 (i)(f) and 14(l)(f), data controllers must therefore inform data subjects about their intent to transfer personal data to IOs. Under Article 15(1)(c), individuals also have a right to learn from data controllers that personal data have or will be disclosed to IOs, and under Article 15(2) they have the right to be informed about the appropriate safeguards that were used for the transfer. What is more according to Articles 44 to 50 of the GDPR, personal data may only be transferred an IO if the latter offers a level of protection that is "essentially equivalent" to that provided within the EU.[74]

GDPR therefore governs possible transfer of personal data from the territory of the EU to IOs located outside the EU.[75] This seems to imply that certain humanitarian IOs would have to comply with GDPR standards in the context of international data transfers, even if they are not party to the GDPR and even if they are not present in the EU's territorial sphere. These GDPR provisions triggered an exchange of letters between the UN Under-Secretary-General for Legal Affairs and the EU delegation to UN. In particular, such extraterritorial or 'back door'[76] application of GDPR was criticized by the UN, which sent comments to the European Data Protection Board, outlining the ways in which the GDPR would be detrimental to organisations in the UN system and raising legal objections to certain aspects of the regulation. The UN stressed the 'adverse impact' the GDPR has had on its activities[77] and urged the EU to "issue additional

---

73 Recital 112, GDPR. See also PIRVAN (n 4).

74 KUNER (n 22), p. 169.

75 See e.g. Chapter V GDPR, see also recitals 107, 108, 112, 153, Articles 12(1)(f), 15(2), 28(3)(a), 30(1)(e), 30(2)(c), 40(2)(j), 40(3), 42(2), GDPR.

76 JERVIS, Claire EM. With WHOm can I share data? Applying the GDPR to transfers of data to International Organisations. EJIL:Talk!, 2020. [online]. Available at: <https://www.ejiltalk.org/with-whom-can-i-share-data-applying-the-gdpr-to-transfers-of-data-to-international-organisations/>. Accessed: 7.8.2024.

77 Ibid.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

guidelines to clarify that the GDPR applies neither to UN-System organizations nor to private entities processing or transferring data on their behalf."[78]

On the other hand, the recently adopted EU AI Act[79] governs the development and use of AI, without prejudice to existing EU law, including data protection and fundamental rights. The AI Act merely complements these existing rules, which therefore continue to apply in the context of the use of AI systems. In terms of substantive provisions, the AI Act is based on the so-called 'risk-based' approach. This means that it categorises AI systems according to the level of risk they might pose from the perspective of health, safety, fundamental rights, the environment, democracy or the rule of law into: prohibited AI practices, high-risk systems listed in Annex III, general-purpose AI models with systemic risk, and general purpose AI models. While AI systems with unacceptable risks are prohibited, high-risk systems are subject to certain requirements in terms of data quality[80], transparency, [81] human oversight, [82] fundamental rights impact assessment[83] and registration. [84] Under the AI Act certain biometric identification[85] systems fall under prohibited practices, e.g. biometric categorisation systems that categorise individually natural persons[86] and 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement (except in certain limited cases).[87] On the other hand, uses of other types of biometrics (e.g. remote biometric identification systems), would have to comply with requirements for high-risk AI systems[88].

Unlike GDPR, the AI Act does not specifically address humanitarian IOs,[89] but it does provide a general exception to the regulation of AI activities:

---

78 BORDIN, Fernando Lusa. Is the EU Engaging in Impermissible Indirect Regulation of UN Action? Controversies over the General Data Protection Regulation. EJIL:Talk!, 2020. [online]. Available at: <https://www.ejiltalk.org/is-the-eu-engaging-in-impermissible-indirect-regulation-of-un-action-controversies-over-the-general-data-protection-regulation/>. Accessed: 7.8.2024.

79 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024 (AI Act).

80 Art. 10, AI Act.

81 Art. 13, AI Act.

82 Art. 14, AI Act.

83 Art. 27, AI Act.

84 Art. 49, AI Act.

85 According to Art. 3(35) AI Act 'biometric identification' means the automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database.

86 Art. 5(1)(g), AI Act.

87 Art. 5(1)(h), AI Act.

88 Section 2, AI Act.

89 Interestingly, it excludes from its scope IOs operating within the EU where an IO uses "AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the Union or with one or more Member States, provided that such a third

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

> This Regulation does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.[90]

However, as is explained in preambular paragraph 24 of the AI Act, the national security exception does not cover humanitarian activities:

> Nonetheless, if an AI system developed, placed on the market, put into service or used for military, defence or national security purposes is used outside those temporarily or permanently for other purposes, for example, civilian or humanitarian purposes, law enforcement or public security purposes, such a system would fall within the scope of this Regulation. In that case, the entity using the AI system for other than military, defence or national security purposes should ensure the compliance of the AI system with this Regulation, unless the system is already compliant with this Regulation.[91]

Against this background, activities of humanitarian IOs falling under the territorial scope of the AI Act, would have to comply with the above-mentioned requirements concerning the use of biometrics. In terms of territorial application the AI Act, like GDPR, includes an extraterritorial dimension. It governs the application and use of AI systems within the EU including for providers[92] and deployers[93] of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the EU.[94] Furthermore, the obligations of the AI Act apply to providers of AI systems that have an effect on the EU – either by placing them on the EU market or putting the AI system into service in the EU. To a certain degree, this seems to extend the application of the EU regulations outside the territory of the EU and to activities of actors outside the EU, including humanitarian IOs.

---

country or international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals." This exception which was arguably included for a particular IO (Europol), is certainly interesting, however, it is not of significant relevance to the work of humanitarian IOs. Art. 2(4) AI Act.

90 Art. 2(3), AI Act.

91 Recital 24, AI Act.

92 A provider within the meaning of the AI Act is any natural or legal person that develops an AI system or a general-purpose AI model (GPAI model) or that has an AI system or a GPAI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge. Art. 3(3) AI Act

93 The role of the deployer applies to organisations **using AI systems** (but not GPAI models) under their authority, which have their place of establishment or are located within the EU. Art. 3(4) AI Act

94 Art. 2(1)(c) AI Act.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

Other regions are beginning to adopt similar data protection regimes. The most notable is the African Union Convention on Cyber Security and Personal Data Protection[95] (Malabo Convention), which entered into force in 2023.[96] Malabo convention includes specific provisions on personal data protection[97] and obliges states to establish legal framework aimed at strengthening fundamental rights, particularly the protection of physical data.[98] It is based on the following fundamental principles: consent and legitimacy of personal data processing, lawful and fair processing of data, collection of data for specific purposes or uses, accuracy of data, transparency of data processing and confidentiality of data.[99] Mirroring the EU regime, data gathering in this legal framework is based on the consent of the data subject, while also foreseeing possible gathering and processing of data in the public interest or in the exercise of official authority and where the processing is necessary to protect the vital interests or fundamental freedoms of the data subject.[100]

However, in contrast to the EU data protection regime, the Malabo Convention does not make any specific mention of humanitarian IOs and does not presuppose the possibility of their accession.[101] Also, it does not include extraterritorial dimensions and only applies to data processing in the territory of its state parties.[102] Consequently, the data protection standards set forth in the Convention are only applicable in the 16 states that are parties to the Convention.[103] This renders the Convention relevant in instances where humanitarian intergovernmental organisations are operating on the territories of these states.

It has been shown in the analysis above, that international and regional data protection and AI legal regimes include provisions relevant to the work of humanitarian IOs, however, the question that remains is the following: are IOs internationally bound by these provisions?

---

95 African Union Convention on Cyber Security and Personal Data Protection (June 2014, entered into force 2023) (Malabo Convention).

96 See also: ECOWAS, Supplementary Act on Personal Data Protection of ECOWAS (February 2010).

97 Arts 9–23, Malabo Convention

98 Art. 8, Malabo Convention

99 Art. 13, Malabo Convention

100 Ibid. ENEYEW AYALEW, Yohannes. The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?. EJIL:Talk!, 2023. [online]. Available at: <https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/?utm_source=mailpoet&utm_medium=email&utm_campaign=ejil-talk-newsletter-post-title_2>.

101 Art. 35, Malabo Convention.

102 Art. 9, Malabo Convention.

103 As of November 2024 26 states have signed and ratified Malabo Convention: Angola, Cape Verde, Côte d'Ivoire, Congo, Ghana, Guinea, Mozambique, Mauritania, Mauritius, Namibia, Niger, Rwanda, Senegal, Sao Tome & Principe, Togo and Zambia.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

4 Humanitarian IOs and Immunities

The question of the applicability and enforceability of the legal regimes analysed above to IOs has been the subject of debate.[104] As already mentioned, IOs are not parties to Convention 108+ and arguably, customary international rules on these issues, which would internationally bind IOs, are yet to crystalize. Humanitarian IOs are therefore not internationally bound by these international standards. However, could humanitarian IOs be held accountable to these standards through the national laws of the states in which they are operating? Similarly, according to relevant EU regulations, humanitarian IOs utilising AI systems for the delivery of aid within the territory of the EU, and on certain occasions also extraterritorially, would have to comply with the EU data protection and AI safeguards. What implications do these provisions have for the work of IOs in practice?

It is argued here that even if the use of AI and processing of data by humanitarian IOs would fall under the material and territorial scope of national or EU laws, the enforcement of these rules is foreclosed by the privileges and immunities to which IOs are entitled to under international law.[105] In essence, these enable IOs to perform their mandates in full independence, whereby they are not covered by the jurisdiction of the countries in which they work.[106] As explained by the European Court of Human Rights in the *Waite and Kennedy* case:

> The attribution of privileges and immunities to international organizations is an essential means of ensuring the proper functioning of such organizations free from unilateral interference by individual governments.[107]

This means that IOs are immune from national legal processes and the enforcement of national or regional data protection frameworks, including the inviolability of records and archives.[108] In other words, even if the use of AI systems and subsequent data processing by IOs falls within the territorial,

---

104 The applicability of GDPR to IOs other than the EU has been subject to discussions, because GDPR itself mentions other international organizations. However, as already explained, without IOs adhering to EU laws, they cannot be considered as being bound by the GDPR. KUNER, Christopher. The GDPR and International Organizations. *AJIL Unbound*, 2020, Vol. 114, pp. 15–19; PIRVAN (n 4).

105 KUNER (n 22), p. 174. Under international law, privileges generally refer to exemptions from the substantive law of a state in areas such as tax and customs, while immunities are exemptions from legal process and immunity from execution and enforcement measures. REINISCH, August. Transnational Judicial Conversations on the Personality, Privileges, and Immunities of International Organizations—An Introduction. In REINISCH, August (ed.). *The Privileges and Immunities of International Organizations in Domestic Courts* Oxford, Oxford University Press, 2013, pp. 6–7. See also REINISCH, August. Accountability of International Organizations According to National Law. *Netherlands Yearbook of International Law*, 2005, Vol. 36, pp. 122–124.

106 KUNER, MARELLI (n 4), p. 81.

107 ECHR, *Case of Waite and Kennedy v. Germany*, (1999) Application no. 26083/94. See also PIRVAN (n 4).

108 Convention on the Privileges and Immunities of the United Nations (1946), UNTS vol. 1, p. 15, and vol. 90, p. 327; Convention on the Privileges and Immunities of Specialized Agencies 81947), UNTS vol. 33, p. 261.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

personal and material scope of relevant national provisions or GDPR and AI Act, their enforcement is foreclosed if such processing is covered by privileges and immunities that they enjoy.[109] This is not novel and was confirmed by scholars[110], IOs themselves[111] as well as the European Data Protection Board (EDPB)[112].

The application of immunities to IOs and the exact scope of immunities that IOs have, has been subject to numerous debates among international legal scholars. In particular, the source of immunities of IOs has not been settled among scholars and courts.[113] According to some, IOs are entitled to immunities under general, customary international law,[114] and some courts have confirmed the existence of certain specific privileges and immunities under customary international law.[115] Others, however, contend that such general customary international legal

---

109 KUNER (n 22), p. 174.

110 Ibid., p. 181 ("IOs typically enjoy immunities against legal process, so that enforcement by a national DPA or court would not be possible against an IO that enjoys immunities with respect to that State. EU law like the *GDPR* becomes part of the legal order of the Member States, and immunities granted on a national level should also apply under the *GDPR* when a DPA or national court conducts enforcement action. Since most enforcement will be carried out at the national level, this means that in practice, IOs will be protected against enforcement by the immunities they enjoy."). See also BORDIN, Fernando Lusa. To what immunities are international organizations entitled under general international law? Thoughts on Jam v IFC and the 'default rules' of IO immunity. *Questions of International Law*, 2020, 72, pp. 5 – 28.

111 "In this regard it is important to note that WFP and other United Nations agencies enjoy certain privileges and immunities, including inviolability of WFP's records and archives under the 1946 Convention on the Privileges and Immunities of the United Nations14 and/or the 1947 Convention on the Privileges and Immunities of Specialized Agencies." WFP Guide to Personal Data Protection and Privacy. WFP, 2016. [online]. Available at: <https://executiveboard.wfp.org/document_download/WFP-0000004049>. Accessed: 7.8.2024, p. 19.

112 "Though not related to the application of Article 3(3), a different situation is the one where, by virtue of international law, certain entities, bodies or organisations established in the Union benefit from privileges and immunities such as those laid down in the Vienna Convention on Diplomatic Relations of 1961, the Vienna Convention on Consular Relations of 1963 or headquarter agreements concluded between international organisations and their host countries in the Union. In this regard, the EDPB recalls that the application of the GDPR is without prejudice to the provisions of international law, such as the ones governing the privileges and immunities of non-EU diplomatic missions and consular posts, as well as international organisations." EUROPEAN DATA PROTECTION BOARD, Guidelines 3/2018 on the territorial scope of the GDPR. 2019. [online]. Available at: at: <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf>. Accessed: 7.8.2024, p. 23.

113 KUNER (n 22), pp. 174–176.

114 See e.g. *Reyes v Al-Malki* [2017] UKSC 61, para 27; Dutch Court of Appeal 's-Hertogenbosch, *Supreme v. Supreme Headquarters Allied Powers Europe (SHAPE)* (2017); Similarly BORDIN (n 110), pp. 5 – 28; REINISCH, August. *International Organisations before National Courts*. Cambridge, Cambridge University Press, 2000, p. 146; SCHERMERS, Henry, BLOKKER, Niels M. *International Institutional Law: Unity within Diversity*. 5th edition. Leiden, The Netherlands: Brill | Nijhoff, 2011, p. 493.

115 For the concrete cases see REINISCH, August. Transnational Judicial Conversations on the Personality, Privileges, and Immunities of International Organizations—An Introduction. In REINISCH, August (ed.). *The Privileges and Immunities of International Organizations in Domestic Courts* Oxford, Oxford University Press, 2013, p. 7, ft 50.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

rules on immunities of IOs have not yet been established.[116] According to this group of scholars, specific immunities of IOs therefore derive from treaty law, i.e. constitutive acts of IOs, headquarters agreements and other bilateral agreements that IOs may sign with states.[117]

Regarding the scope and nature of immunities of IOs, some authors advocate for a distinction under general international law, between immunities of states and IOs,[118] the latter being limited with functions of IOs.[119] Such functional immunities mean that IOs enjoy such immunities as are "necessary to for the exercise of their functions in the fulfilment of their purposes."[120] On the other hand, others advocated for an analogous application of immunities of States to that of IOs, including the *jure gestionis* and *jure imperii* distinction.[121]

It is not the aim of this chapter to further dwell on these issues. In passing, however, it is worth mentioning that the better understanding of immunities of IOs seems to be the one that derives the entitlement to immunities by IOs from the general international law (and not by virtue of their internal law or treaty law).[122] This would mean that all IOs (as international legal subjects) have the capacity to be immune from national laws, an entitlement, which derives from their international legal personality. In a similar way as IOs enjoy treaty making capacity and capacity to react to a breach of international law and to be subject of responsibility, they also enjoy the capacity to be subject to immunities. On the other hand, the extent to which such immunities are to be actually acknowledged is to be determined by the internal rules of a particular IO (especially constitutive acts) or other international treaties, as immunities essentially depend upon

116 SANDS, Philippe, KLEIN, Pierre. *Bowett's Law of International Institutions*. 6th edition. Sweet & Maxwell, 2009, p. 493; WOOD, Michael. Do International Organizations Enjoy Immunity under Customary International Law?. *International Organizations Law Review*, Vol. 10, Issue 2, p. 317.

117 E.g. Convention on Privileges and Immunities of the United Nations, 1 UNTS 15 and 90, p. 372 (entered into force 17 September 1946).

118 CHAN, Caleb Edward. International Organisation Immunity from Execution before the Dutch Court of Appeal: Some Observations on *Supreme v. SHAPE*. Jus Cogens: The International Law Podcast & Blog, 2022. [online]. Available at: <https://juscogens.law.blog/2022/09/02/international-organisation-immunity-from-execution-before-the-dutch-court-of-appeal-some-observations-on-supreme-v-shape/>. Accessed 7.8.2024.

119 See e.g. Art. 105(1) of the Charter of the United Nations (UN Charter) (Opened for signature 24 June 1945, entered into force 24 October 1945) 1 UNTS XVI; KUNER (n 22), p. 175.

120 KLABBERS, Jan. *An Introduction to International Organizations Law*. Cambridge, Cambridge University Press, 2015, p. 131.

121 BORDIN (n 110), pp. 5 – 28.

122 This is supported by: *Reyes v Al-Malki* [2017] UKSC 61, para 27; Dutch Court of Appeal 's-Hertogenbosch, *Supreme v. Supreme Headquarters Allied Powers Europe (SHAPE)* (2017); Similarly BORDIN (n 110), pp. 5 – 28; REINISCH, August. *International Organisations before National Courts*. Cambridge: Cambridge University Press, 2000, p. 146; SCHERMERS, Henry, BLOKKER, Niels M. *International Institutional Law: Unity within Diversity*. 5th edition. Leiden, The Netherlands: Brill | Nijhoff, 2011, p. 493. For a contrary view, that there does not exist customary international legal rules on immunities of IOs see: SANDS, KLEIN (n 116), p. 493; WOOD (n 116), p. 317.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

the functions and purposes of the concerned IO.[123] For the purposes of our discussions, however, it suffices to make two substantive remarks concerning the immunities of WFP.

First, in terms of sources, regardless of the existence of IOs immunities under customary international law, the UN and its specialized agencies, including WFP, enjoy immunities as delineated in the following multilateral treaties: the UN Charter[124], the Convention on the Privileges and Immunities of the United Nations[125] and the Convention on the Privileges and Immunities of the Specialised Agencies[126]. According to these, WFP is immune from national legal processes, including those relating to data protection and AI regulation.[127] As has been observed by Kuner, not only states, but also the EU itself is bound to observe the immunities of UN and its specialized agencies deriving from international law[128], even if it is not a party to these conventions. This is the case because of its duty not to interfere with the international obligations of its member states towards these IOs, or because the international obligations of its member states became binding on the EU itself,[129] or because these obligations are part of customary international law. In terms of the relationship between EU's international obligations (concerning immunities of IOs) and fundamental rights as embedded in EU primary law (including data protection) recent practice of the Court of Justice of the EU, seems to conform to the autonomy of the EU law, thus giving precedence to relevant European fundamental rights, over international obligations.[130] It is therefore not entirely clear, whether and how would the Court of Justice of the EU decide when/if confronted with the application of immunities to humanitarian IOs falling under the material and territorial scope of its data protection regulations. From an international law perspective, however, the immunities of UN specialised agencies, as previously described, are relatively straightforward and therefore foreclose the application of the relevant EU data protection and AI provisions.

---

123 For an in depth analysis of a relationship between the international legal personality, capacities and competences of IOs see T. VEBER, Maruša. Sanctions Adopted by International Organizations in the Defence of the General Interest. PhD Thesis, University of Ljubljana, 2022, pp. 153–173.

124 Art. 105, UN Charter.

125 Convention on Privileges and Immunities of the United Nations, 1 UNTS 15 and 90, p. 372 (entered into force 17 September 1946).

126 Convention on the Privileges and Immunities of the Specialised Agencies, UNTS 33, p. 261 (entered into force 2 December 1948).

127 Art. II, Convention on the Privileges and Immunities of the United Nations; Article III Convention on the Privileges and Immunities of the Specialised Agencies.

128 See HEUNINCKX, Baudouin, *The Law Of Collaborative Defence Procurment in the European Union*. Cambridge: Cambridge University Press, 2017, p. 153–155.

129 KUNER (n 22), pp. 178–179.

130 See e.g. 402/05 and C-415/05, *Yassin Abdullah Kadi and Al Barakaat International Foundation* v. *Council of the European Union and the Commission of the European Communities* (2008) ECLI:EU:C:2008:461 (*Kadi* I 2008), para. 285; Case C-284/16, *Slowakische Republik v Achmea BV* (2018), ECLI:EU:C:2018:158, paras. 33, 41, 59.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

Secondly, regardless of which of the two approaches one undertakes concerning the scope of immunities of IOs, the activities of WFP, when delivering humanitarian aid in the aftermath of natural or man-made disasters, would seem to fall under the category of acts of IOs that are covered by immunities (either by the functional theory or because these acts qualify as *acta jure imperii*).

It has to be acknowledged, however, that even though relevant GDPR and AI Act provisions are not directly enforceable in relation to the work of IOs on the account of immunities, there nevertheless exists an informal pressure for them to comply with these provisions to a certain extent. As was explained above with regard to the international data transfers to IOs, the EU-based controllers and processors would have to make sure that such transfers take place in accordance with GDPR provisions.[131] In practice, therefore, IOs may be subject to informal pressure to adopt EU data protection standards, through the use of conditionality or soft enforcement. Data exporters in the EU may themselves therefore be pressured to ensure that the data they transfer receive adequate protection, which could result in them obliging IOs that receive data from the EU, to implement suitable safeguards. The European Commission has also indicated informally that data transfers to IOs outside the European Economic Area can only be carried out in accordance with EU data protection law.[132]

Indeed, this conditionality of the EU legal regimes has had a profound informal influence on the internal data protection regulation of humanitarian IOs and the EU AI act is likely to have a similar impact on the internal AI-related provisions of humanitarian IOs. However, as described above, the enforcement of EU legal data protection and AI legal regimes in relation to the work of humanitarian IOs, e.g. the WFP, is precluded on the basis of immunities. Against this background, the most important legal regimes governing the work of humanitarian IOs are their internal data protection and AI policies and regulations.

5 Internal Data Protection and AI Legal Regimes and the Role of Individual Consent

Due to IOs' increasing use of AI and data-intensive technologies in practice, whereby "misuse of personal data may have life and death consequences",[133] there was a growing need for the development and implementation of internal data protection rules by IOs, which to a large extent mirror the existing international and regional regimes.

At the UN level, the first document explicitly addressing data protection are the 1990 UN General Assembly Guidelines for the Regulation of Computerized

131 EUROPEAN DATA PROTECTION BOARD (n 112).

132 KUNER (n 22), p. 182.

133 KUNER (n 104), p. 15. Indeed, in the context of international humanitarian organizations, it is crucial for their work to work "as effectively and efficiently as possible to assist vulnerable individuals fleeing persecution or involved in natural disasters, so that protecting their processing of personal data can literally be a matter of life and death." KUNER (n 22), p. 162

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

Personal Data Files,[134] which include among others the principles of lawfulness and fairness, accuracy, purpose-specification and security of data files. The guidelines apply to the UN and its specialized agencies.[135] At the same time, however, they allow for a 'humanitarian derogation' from these principles when the purpose of derogation is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance.[136] Other important developments at the UN level include the UN General Assembly Resolution affirming the right to privacy in the digital age,[137] appointment in 2016 of a Special Rapporteur on the Rights to Privacy in 2015[138] and the establishment of the UN Privacy Policy Group (UNPPG) in 2016, the primary objective of which is the sharing of information on data protection within the UN system. UNPPG developed the UN Principles on Personal Data Protection and Privacy,[139] a non-binding document encouraging the UN system organizations to adhere to the following ten principles when processing personal data in carrying out their mandated activities: fair and legitimate processing; purpose specification; proportionality and necessity; retention; accuracy; confidentiality; security; transparency; transfers and accountability.[140] Following the COVID-19 pandemic UNPPG also developed the Joint Statement on Data Protection and Privacy in Response to COVID-19 to reinforce the UN's commitment to using data and technology in a way that respects human rights by the UN specialized agencies, including WFP.[141] In other documents, such as the 2020–2022 Data Strategy of the UN Secretary-General, data protection is listed among 12 core data principles.[142]

Moreover, to adapt to the increasing use of AI by the UN and its specialized agencies, the Principles for the Ethical Use of Artificial Intelligence in the United Nations System were adopted in 2022,143 which are based on the UNESCO

---

134 Guidelines for the Regulation of Computerized Personal Data Files, UNGA Resolution 5/95 of 14 December 1990.

135 Part V, ibid.

136 Ibid.

137 UNGA Resolution, The right to privacy in the digital age, UN Doc. A/RES/71/199 (25 January 2017).

138 UNITED NATIONS DEVELOPMENT PROGRAMME. Compendium of Data Protection and Privacy Policies and Other Related Guidance Within the United Nations Organization and Other Selected Bodies of the International Community. 2021. [online]. Available at: <https://unstats.un.org/legal-identity-agenda/documents/Paper/data_protecton_%20and_privacy.pdf>. Accessed: 7.8.2024, p. 13.

139 UN High-Level Committee on Management (HLCM), Personal Data Protection and Privacy Principles, 11 October 2018.

140 Ibid.; KUNER (n 104), pp. 15–19.

141 UNITED NATIONS. Joint Statement on Data Protection and Privacy in the COVID-19 Response. 2020. [online]. Available at: <https://www.un.org/en/coronavirus/joint-statement-data-protection-and-privacy-covid-19-response>.

142 Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity 2020–2022, p. 19. For a comprehensive overview of UN policies in the area of data protection and privacy see UNITED NATIONS DEVELOPMENT PROGRAMME (n 138).

143 UN SYSTEM CHIEF EXECUTIVES BOARD FOR COORDINATION. Principles for the Ethical Use of Artificial Intelligence in the United Nations System. 2022. [online]. Available at: <https://

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

Recommendation on the Ethics of Artificial Intelligence.[144] This set of ten principles, grounded in ethics and human rights, aims to guide the use of AI across all stages of an AI system lifecycle by UN system entities. It includes the following principles: do no harm; defined purpose, necessity and proportionality; safety and security; fairness and non-discrimination; sustainability; right to privacy, data protection and data governance; human autonomy and oversight; transparency and explainability; responsibility and accountability; and inclusion and participation. These principles provide the key framework on the use of AI systems within the UN. Another important document is the March 2024 UNGA Resolution on AI stressing the need for the use and development of safe, secure and trustworthy AI systems which are human-centric, reliable, explainable, ethical, inclusive, privacy-preserving and which promote and protect human rights and international law.[145] The UNGA in particular, stressed the importance of data protection throughout the lifecycle of AI systems and emphasized that:

> [h]uman rights and fundamental freedoms must be respected, protected and promoted throughout the life cycle of artificial intelligence systems, calls upon all Member States and, where applicable, other stakeholders to refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights, especially of those who are in vulnerable situations, and reaffirms that the same rights that people have offline must also be protected online, including throughout the life cycle of artificial intelligence systems.[146]

On the basis of these developments at the UN level, specialized agencies themselves developed their specific internal data protection policies,[147] however, they have yet to adopt their internal AI-related provisions.

For example, WFP is committed to addressing the risks posed by data collection and use to the people it serves,[148] while embracing digitalization as a key driver of innovative and more efficient hunger solutions and capitalizing "on the power of data to help us make the most of limited resources and ensure they are directed to those in urgent need."[149] WFP therefore adopted its Humanitarian Protection Policy[150] which unequivocally requires that food and nutrition assistance be

---

unsceb.org/principles-ethical-use-artificial-intelligence-united-nations-system#:~:text=It%20is%20intended%20to%20be,data%20governance%3B%20human%20autonomy%20and>.

144 UNESCO (n 2).

145 UNGA Resolution A/78/L.49, 11 March 2024.

146 Ibid., para. 5.

147 UNHCR. Policy on the Protection of Personal Data of Persons of Concern to UNHCR. 2015. [online]. Available at: < https://www.refworld.org/policy/strategy/unhcr/2015/en/120873>. Accessed: 7.8.2024.

148 WFP strategic plan (n 14), para. 131.

149 WFP Global Data Strategy (n 12).

150 WFP Humanitarian Protection Policy. WFP/EB.1/2012/5-B/Rev.1, 15 February 2012.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

delivered with respect to human rights and that food assistance should contribute to the safety, dignity and integrity of vulnerable people. Moreover, the WFP has its own privacy policy and a Guide to Personal Data Protection and Privacy,[151] which includes the necessity of conducting the Privacy Impact Assessment (PIA):

> Prior to data processing WFP shall engage in a Privacy Impact Assessment (PIA). A PIA is a privacy-specific risk-benefit analysis aimed at weighing the probability of harm against the anticipated benefits, and ensuring that the benefits significantly outweigh the potential risks and that any identified risks are avoided or mitigated. This includes considerations for the safety of WFP personnel.[152]

In terms of security, principle 5 stipulates that:

> WFP shall continue to implement appropriate physical, organizational and technological security measures to protect personal data against accidental loss and/or damage, unauthorized access, disclosure, modification and destruction, and to ensure continuous availability of WFP's application programs and data.

Generally, the WFP data protection policy is based on five principles: lawful and fair collection and processing; specified and legitimate purpose; data quality; participation and accountability and data security.[153] Central to the WFP data protection policy is the informed consent of the beneficiary[154]: when gathering and processing personal data, the consent of an individual must always be obtained, whether explicitly or implicitly,[155] whereas individuals may withhold or withdraw their consent at any time. Explicit consent may be obtained in writing, through a statement verbally released by beneficiaries, individually or collectively. On the other hand, the consent may also be implicit, as long as the beneficiary has received all the required information; there is no evident obstacle to the expression of his/her free will; he/she has not put forward any objection after having been given the opportunity to do so.[156] To comply with the informed consent requirement WFP is to provide certain information on data gathering and processing, which include: the identity and mandate of the data collector and data controller; types of personal data collected/used; reasons for gathering personal data; information on possible sharing of data; information as to how to access, update, modify, correct or delete data and how to access complaint procedures; the beneficiary's right to

151 WFP Guide to Personal Data Protection and Privacy (n 111).
152 Ibid., p.15.
153 Ibid., pp. 16–17.
154 Ibid., pp. 46–55.
155 Ibid., p. 22.
156 Ibid., p. 47.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

refuse to provide the information, and the implications of withholding consent.[157] The latter is important, as a possible beneficiary's refusal to provide the required information may make it impossible for WFP to assist.

It is questionable, however, whether AI solutions used by the WFP, including biometric identification such as iris scanning, comply with these internal data protection provisions, e.g. security, do-no-harm principle and impartiality.[158] The applicability of the existing data protection regimes to AI solutions is often questioned because AI technically enables the processing of large amounts of data. Moreover, due to the complexities of AI systems, certain data protection requirements such as security, explainability and tracing of data are difficult to comply with. Applying data protection principles and rights of data subjects such as the right to be informed about the use of AI, the purpose and the legal basis of processing their rights as data subjects, and the risks, rules and safeguards concerning processing of their data[159] to AI solutions has been considered as challenging,[160] including by the High Commissioner for Human Rights[161] and in relation to biometric identification and counterterrorism policies.[162]

More importantly, it is questionable whether the WFP's consent–centered data policies, which seem to provide a broad legal basis for gathering and processing of personal data, are suitable in a humanitarian context whereby it is often difficult to establish informed and freely given consent in accordance with the data protection rules. In light of the CoE and GDPR data protection standards, the more appropriate legal basis would seem to be either the vital interest of the data subject and reasons of public interest.[163] Therefore, rather than focusing on the implicit or explicit consent of an individual in a humanitarian context, the focus should rather be on the development of incorporating sufficient safeguards for data protection and safe use of AI to prevent possible misuse of data and human rights more generally. This seems to have been acknowledged in the WFP Global Data Strategy 2024–2026:

157 Ibid., p. 49.
158 NARBEL, SUKAITIS (n 4).
159 KUNER, MARELLI (n 4), pp. 290–292.
160 See Ibid., p. 283 ff.
161 Report of the High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc. A/HRC/48/31, 15 September 2021.
162 UN Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counterterrorism. [online]. Available at: <https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_on_biometricsl_eng.pdf>. Accessed: 4.8.2024.
163 UNHCR (n 147), p. 15. GDPR, para 12 for example allows for the transfer of personal data to an international humanitarian organisation, "with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject." See also KUNER (n 104), pp. 15–19.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

> Our success will be determined by the implementation of fundamental principles of data security and data protection essential to WFP's mission. These safeguards are vital to reduce the risks that come with processing data in humanitarian contexts, where vulnerable individuals and communities can fall prey to exploitation or harm.[164]

Indeed, organizations such as the UNHCR allow for data gathering on a legitimated basis other than consent, i.e. vital or best interests of the data subject.[165] Moreover, ICRC adopted specific policies on the processing of biometric data, whereby the legitimate basis for the use of such systems derives either from the important grounds of public interest or the legitimate interest of the ICRC, and not the consent of individuals, with the emphasis on the various safeguards such as the data protection impact assessment and certain security features (e.g. encryption of data at rest and in transit to minimise the risk of unauthorised access; prevention of unauthorised disclosure of biometric data using technical means including the 'one way encoding')[166] and non-sharing or otherwise transfer biometric data to any government or authorities.

6 Concluding remarks

This paper has shown that humanitarian IOs increasingly rely on AI systems to fulfil their humanitarian mandates. The focus was on the practice of the WFP, which commonly uses AI technology, including biometric systems in the delivery of aid. As humanitarian IOs process increased amounts of personal data, they cannot expect to be completely isolated from the growing importance of data protection,[167] which brings to the fore the question of which data protection and AI legal regimes govern their activities. Focusing specifically on relevant EU legislation, it was explained that because IOs are not parties of relevant international and regional data protection and AI legal regimes and on the account of immunities to which IOs are entitled to under the general international law, the enforcement of these standards in relation to their work is foreclosed. In light of this, and due to IOs' increasing use of AI and data-intensive technologies in practice, there was a growing need for the development and implementation of relevant internal rules by IOs. While humanitarian IOs, such as the WFP developed their internal data protection policies, they have yet to adopt similar AI related policies.

This paper highlighted two limitations deriving from the WFP's data protection policies. First, it is questionable whether AI solutions used by the

164 WFP Global Data Strategy (n 12), p. 3.

165 UNHCR (n 147), p. 15.

166 Policy on the Processing of Biometric Data by the ICRC. 2019. [online]. Available at: <https://www.icrc.org/sites/default/files/document/file_list/icrc_biometrics_policy_adopted_29_august_2019_.pdf>. Accessed: 4.8.2024.

167 BARBOZA, JASMONTAITĖ-ZANIEWICZ, DIVER (n 5), p. 164.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

WFP, including biometric identification such as iris scanning, comply with its internal data protection provisions, e.g. security, do-no-harm principle and impartiality. Second, while WFP data protection policies to a large extend draw from the standards included in the international and EU data protection regimes, there nevertheless exist important differences. In particular, WFP's data protection policy centres on the notion of individual consent, even though it has been acknowledged that in the emergency situations, in which humanitarian IOs typically operate, obtaining valid, informed and freely given consent is often difficult. In such situations IOs could rely on two alternative legal bases: the vital interest of the data subject or reasons of public interest. Simultaneously, however, the future focus of internal policies of humanitarian IOs should be on the development of sufficient safeguards for data protection and safe use of AI thereby protecting beneficiaries and their human rights when interacting with these organizations.

List of references

BAKER, Fran, ETYEMEZIAN, Hovig, MORENO JIMÉNEZ, Rebeca. AI for efficient, evidence-informed humanitarianism. UNHCR Innovation Service, 2024. [online]. Available at: <https://medium.com/unhcr-innovation-service/ai-for-efficient-evidence-informed-humanitarianism-fd246238a0ad>. Accessed: 7.8.2024.

BEDUSCHI, Ana. Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks. *International Review of the Red Cross,* 2022, vol. 104 issue 919, pp. 1149–1169.

BORDIN, Fernando Lusa. Is the EU Engaging in Impermissible Indirect Regulation of UN Action? Controversies over the General Data Protection Regulation. EJIL:Talk!, 2020. [online]. Available at: <https://www.ejiltalk.org/is-the-eu-engaging-in-impermissible-indirect-regulation-of-un-action-controversies-over-the-general-data-protection-regulation/>. Accessed: 7.8.2024.

BORDIN, Fernando Lusa. To what immunities are international organizations entitled under general international law? Thoughts on Jam v IFC and the 'default rules' of IO immunity. *Questions of International Law*, 2020, vol. 72, pp. 5–28.

BRKAN, Maja. The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal*, 2019, Volume 20, Special Issue 6, pp. 864–883.

CENTRE FOR INFORMATION POLICY LEADERSHIP. Artificial Intelligence and Data Protection in Tension, First Report, 2018. [online]. Available at: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf>. Accessed: 7.8.2024.

CHAN, Caleb Edward. International Organisation Immunity from Execution before the Dutch Court of Appeal: Some Observations on *Supreme v. SHAPE*. Jus Cogens: The International Law Podcast & Blog, 2022. [online]. Available at: <https://juscogens.law.blog/2022/09/02/international-organisation-immunity-from-execution-before-the-dutch-court-of-appeal-some-observations-on-supreme-v-shape/>. Accessed 7.8.2024.

DIGGELMANN, Oliver, CLEIS, Maria Nicole. How the Right to Privacy Became a Human Right. *Human Rights Law Review*, 2014, Vol. 14, Issue 3, pp. 441–458.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

ENEYEW AYALEW, Yohannes. The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?. EJIL:Talk!, 2023. [online]. Available at: <https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/?utm_source=mailpoet&utm_medium=email&utm_campaign=ejil-talk-newsletter-post-title_2>. Accessed: 7.8.2024.

EUROPEAN DATA PROTECTION BOARD, Guidelines 3/2018 on the territorial scope of the GDPR. 2019. [online]. Available at: at: <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf>. Accessed: 7. 8. 2024.

EUROPEAN DATA PROTECTION BOARD. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. 2022. [online]. Available at: <https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf >. Accessed: 20.4.2023.

FORDE, Aidan. The Conceptual Relationship between Privacy and Data Protection. *Cambridge Law Review*, 2016, Issue 1, pp. 135–149.

FRA. Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2020. Available at: <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf>. Accessed: 7.8.2024.

HEUNINCKX, Baudouin, *The Law Of Collaborative Defence Procurment in the European Union*. Cambridge: Cambridge University Press, 2017.

HILDEBRANDT, Mireille. *Law for Computer Scientists and Other Folk*. Oxford, Oxford University Press, 2020.

JERVIS, Claire EM. With WHOm can I share data? Applying the GDPR to transfers of data to International Organisations. EJIL:Talk!, 2020. [online]. Available at: <https://www.ejiltalk.org/with-whom-can-i-share-data-applying-the-gdpr-to-transfers-of-data-to-international-organisations/>. Accessed: 7.8.2024.

KAYHAN, Halid. Using Biometrics to Provide Humanitarian Aid… While the 'data hunt' to identify "security threats" is on the rise?! (PART I). [online]. Available at: <https://www.law.kuleuven.be/citip/blog/using-biometrics-to-provide-humanitarian-aid-part-i/>. Accessed: 7.8.2024.

KITTICHAISAREE, Kriangsak, KUNER, Christopher. The Growing Importance of Data Protection in Public International Law. EJIL:Talk!, 2015. [online]. Available at: <https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/>. Accessed: 7.8.2024).

KLABBERS, Jan. *An Introduction to International Organizations Law*. Cambridge, Cambridge University Press, 2015.

KUNER, Christoper, MARELLI, Massimo. *Handbook on Data Protection in Humanitarian Action. Second edition*. ICRC. [online]. Available at: <https://www.icrc.org/en/data-protection-humanitarian-action-handbook>. Accessed: 5.5.2024.

KUNER, Christopher. International Organizations and the EU General Data Protection Regulation: Exploring the Interaction between EU Law and International Law. *International Organizations Law Review*, 2019, vol. 16, no. 1, pp. 158–191.

KUNER, Christopher. The GDPR and International Organizations. *AJIL Unbound*, 2020, Vol. 114, pp. 15–19.

LATONERO, Mark. Stop Surveillance Humanitarianism. New York Times, 2019. [online]. Available at: <https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html>. Accessed: 10.8.2024.

LINDBLOM, Anna-Karin. *Non-Governmental Organisations in International Law*. Cambridge, Cambridge University Press, 2009.

MACDONALD, Ayang. African nations must implement safeguards against humanitarian digital ID risks: researcher. Biometric update, 2022. [online]. Available at: <https://www.biometricupdate.com/202209/african-nations-must-implement-safeguards-against-humanitarian-digital-id-risks-researcher>. Accessed: 20.4.2024.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

MADIANOU, Mirca. Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises. *Social Media & Society*, 2019, Vol.5, No. 3.

MARTIN, Aaron, SHARMA, Gargi, DE SOUZA, Siddarth Peter, TAYLOR, Linnet, VAN EERD, Boudewijn, MCDONALD, Sean Martin, MARELLI, Massimo, CHEESMAN, Margie, SCHEEL, Stephan, DIJSTELBLOEM, Huub. Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions. *Geopolitics,* 2023, Vo. 28, No. 3, pp. 1363–1397.

NARBEL, Vincent Graf, SUKAITIS, Justinas. Biometrics in humanitarian action: a delicate balance. *Humanitarian Law & Policy*, 2021. [online]. Available at: <https://blogs.icrc.org/law-and-policy/2021/09/02/biometrics-humanitarian-delicate-balance/>. Accessed: 20.4.2023.

Palantir Ranked No. 1 in Worldwide Artificial Intelligence Software Study in Market Share and Revenue. Businesswire, 2022. [online]. Available at: <https://www.businesswire.com/news/home/20220920006178/en/Palantir-Ranked-No.-1-in-Worldwide-Artificial-Intelligence-Software-Study-in-Market-Share-and-Revenue>. Accessed: 20.8.2024.

PARKER, Ben. Audit exposes UN food agency's poor data-handling. The New Humanitarian, 2018. [online]. Available at: <https://www.thenewhumanitarian.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling>. Accessed: 7.8.2024.

PARKER, Ben. New UN deal with data mining firm Palantir raises protection concerns. The New Humanitarian, 2019. [online]. Available at: <https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp>. Accessed: 20.4.2024.

PIRVAN, Petruta. EU GDPR applicability to international organizations. iapp, 2021. [online]. Available at: <https://iapp.org/news/a/eu-gdpr-applicability-to-international-organizations/>. Accessed: 7.8. 2024.

Policy on the Processing of Biometric Data by the ICRC. 2019. [online]. Available at: <https://www.icrc.org/sites/default/files/document/file_list/icrc_biometrics_policy_adopted_29_august_2019_.pdf>. Accessed: 4.8.2024.

REINISCH, August. Accountability of International Organizations According to National Law. *Netherlands Yearbook of International Law*, 2005, Vol. 36, pp. 119–167.

REINISCH, August. *International Organisations before National Courts*. Cambridge, Cambridge University Press, 2000.

REINISCH, August. Transnational Judicial Conversations on the Personality, Privileges, and Immunities of International Organizations—An Introduction. In REINISCH, August (ed.). *The Privileges and Immunities of International Organizations in Domestic Courts* Oxford, Oxford University Press, 2013.

SANDS, Philippe, KLEIN, Pierre. *Bowett's Law of International Institutions*. 6th edition. Sweet & Maxwell, 2009.

SCHERMERS, Henry, BLOKKER, Niels M. *International Institutional Law: Unity within Diversity*. 5th edition. Leiden, The Netherlands: Brill | Nijhoff, 2011.

SLIM, Hugo. Eye Scan Therefore I am: The Individualization of Humanitarian Aid. European University Institute, 2015. [online]. Available at: <https://iow.eui.eu/2015/03/15/eye-scan-therefore-i-am-the-individualization-of-humanitarian-aid/>. Accessed 7.8.2024.

T. VEBER, Maruša. AI-Supported Humanitarian Aid and the Right to Life: Highlighting Some of the Legal Challenges Faced by International Humanitarian Organizations. In: SANCIN, Vasilka (ed.). *Artificial Intelligence and Human Rights: From the Right to Life to Myriad of Diverse Human Rights Implications*. Ljubljana, Litteralis 2025 (forthcoming).

T. VEBER, Maruša. Artificial Intelligence and Humanitarian Assistance: Reassessing the Role of State Consent. *Ljubljana Law Review*, 2024, vol. 84, pp. 217–253.

T. VEBER, Maruša. Sanctions Adopted by International Organizations in the Defence of the General Interest. PhD Thesis, University of Ljubljana, 2022.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)

TIEDRICH, Lee, CAIRA, Celine, BENHAMOU, Yaniv. The AI data challenge: How do we protect privacy and other fundamental rights in an AI-driven world?. OECD AI Policy Observatory, 2023. [online]. Available at: <https://oecd.ai/en/wonk/the-ai-data-challenge-how-do-we-protect-privacy-and-other-fundamental-rights-in-an-ai-driven-world>. Accessed: 7.8.2024.

UN Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counterterrorism. [online]. Available at: <https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_on_biometricsl_eng.pdf>. Accessed: 4.8.2024.

UN food chief warns aid suspension in Yemen likely to start this week. Reuters, 2019. Available at: <https://www.reuters.com/article/us-yemen-security-un/u-n-food-chief-warns-aid-suspension-in-yemen-likely-to-start-this-week-idUSKCN1TI1X7>. Accessed: 20.8.2024.

UN SYSTEM CHIEF EXECUTIVES BOARD FOR COORDINATION. Principles for the Ethical Use of Artificial Intelligence in the United Nations System. 2022. [online]. Available at: <https://unsceb.org/principles-ethical-use-artificial-intelligence-united-nations-system#:~:text=It%20is%20intended%20to%20be,data%20governance%3B%20human%20autonomy%20and>.

UNESCO Recommendation on the Ethics of Artificial Intelligence. [online]. Available at <https://unesdoc.unesco.org/ark:/48223/pf0000380455>. Accessed: 1.1.2024.

UNHCR. Policy on the Protection of Personal Data of Persons of Concern to UNHCR. 2015. [online]. Available at: < https://www.refworld.org/policy/strategy/unhcr/2015/en/120873>. Accessed: 7.8.2024.

UNITED NATIONS DEVELOPMENT PROGRAMME. Compendium of Data Protection and Privacy Policies and Other Related Guidance Within the United Nations Organization and Other Selected Bodies of the International Community. 2021. [online]. Available at: <https://unstats.un.org/legal-identity-agenda/documents/Paper/data_protecton_%20and_privacy.pdf>. Accessed: 7.8.2024.

UNITED NATIONS. Joint Statement on Data Protection and Privacy in the COVID-19 Response. 2020. [online]. Available at: <https://www.un.org/en/coronavirus/joint-statement-data-protection-and-privacy-covid-19-response>.

WATT, Eliza. *State Sponsored Cyber Surveillance, The Right to Privacy of Communications and International Law*. Edward Elgar Publishing, 2021.

WFP Global Data Strategy 2024–2026. [online]. Available at: <https://reliefweb.int/report/world/wfp-global-data-strategy-2024-2026>. Accessed: 7.8.2024.

WFP Guide to Personal Data Protection and Privacy. WFP, 2016. [online]. Available at: <https://executiveboard.wfp.org/document_download/WFP-0000004049>. Accessed: 7.8.2024.

WFP Introduces Iris Scan Technology To Provide Food Assistance To Syrian Refugees In Zaatari. WFP, 2016. [online]. Available at: < https://reliefweb.int/report/jordan/wfp-introduces-iris-scan-technology-provide-food-assistance-syrian-refugees-zaatari>. Accessed: 20.8.2024.

WFP strategic plan (2022–2023). WFP/EB.2/2021/4-A/1/Rev.2, 12 November 2021.

WOOD, Michael. Do International Organizations Enjoy Immunity under Customary International Law?. *International Organizations Law Review*, Vol. 10, Issue 2, pp. 287–318.

ZALNIERIUTE, Monika. An international constitutional moment for data privacy in the times of mass-surveillance. *International Journal of Law and Information Technology*, 2015, Vol. 23, Issue 2, pp. 99–133.

ZOMIGNANI BARBOZA, Julia, JASMONTAITĖ-ZANIEWICZ, Lina, DIVER, Laurence. Aid and AI: The Challenge of Reconciling Humanitarian Principles and Data Protection. *14th IFIP International Summer School on Privacy and Identity Management (Privacy and Identity)*. 2019, Windisch, Switzerland.

Published by Palacký University Olomouc, Czech Republic, 2024.
ISSN 1213-8770 (print); ISSN 2464-6601 (online)