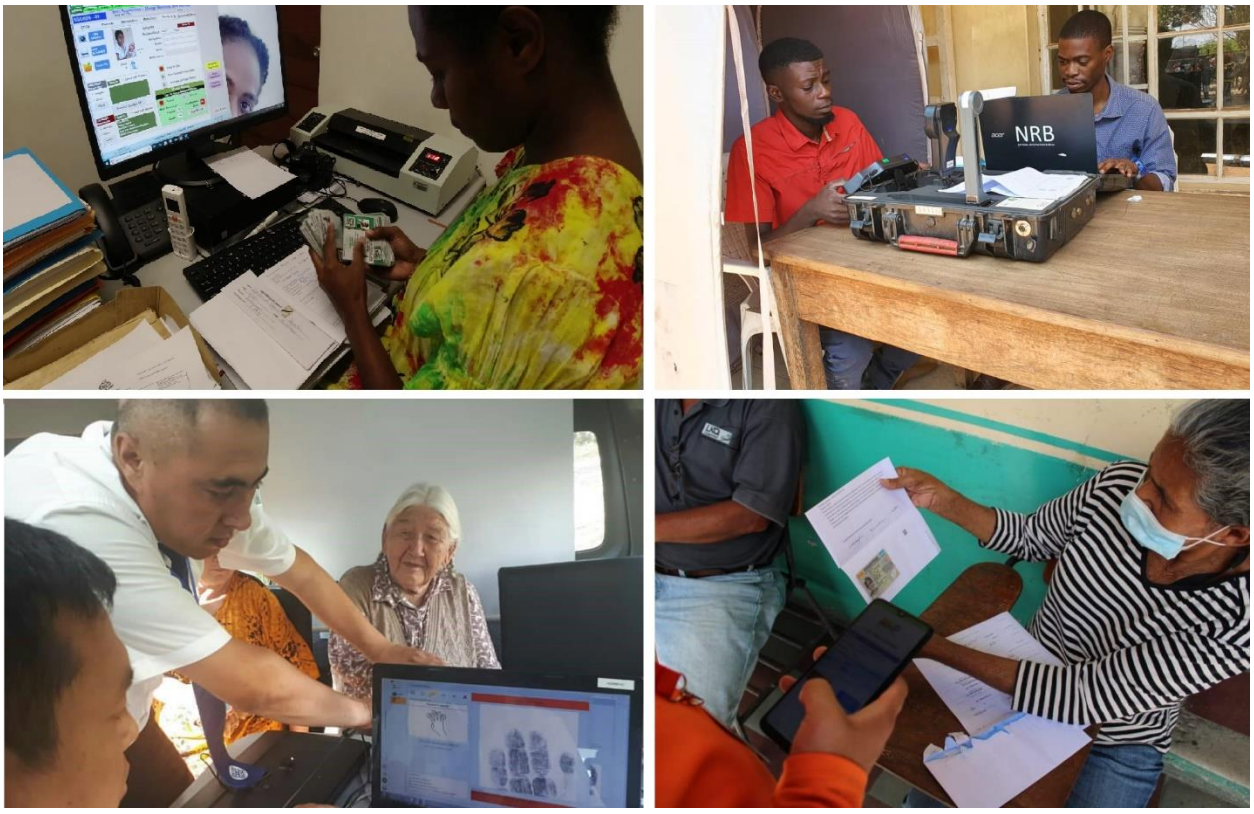
Empowered lives.
Resilient nations.

COMPENDIUM OF DATA PROTECTION AND PRIVACY POLICIES AND OTHER RELATED GUIDANCE WITHIN THE UNITED NATIONS ORGANIZATION AND OTHER SELECTED BODIES OF THE INTERNATIONAL COMMUNITY

November 2021



This product is produced with the kind contribution from:

From the People of Japan

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development and Cooperation SDC

Sida

This material/production has been financed by the Swedish International Development Cooperation Agency, Sida. Responsibility for the content rests entirely with the creator. Sida does not necessarily share the expressed views and interpretations.

Contents

1. INTRODUCTION

1.1 Purpose and Scope

The purpose of this Compendium is to 'map' UN policy in the area of data protection and privacy (as well as identify some correspondent key data protection and privacy-related texts among international organisations outside the UN system).[1] This includes a review of:

- the current UN normative framework – essentially treaty/convention level texts that bind UN Member States, as well as Resolutions of various Member State organs of the UN and the reports of senior UN officials that preceded them;
- non-normative, inter-agency digital and data strategies/initiatives – (such as the Secretary-General's Data Strategy) that aim to guide/advise either the UN system or Member States on broad digital and data transformation that include data protection and privacy dimensions;
- internal privacy and data protection policies of selected UN entities – including those agencies (primarily, though not exclusively, UNHCR and WFP) that process personally-identifying information (PII) of their client populations;
- advisory and technical assistance activity of the UN and other selected bodies within the international community in support of data protection and privacy legislative and institutional governance frameworks, particularly in the health, identity and commercial spheres.

Although the impetus to compile this compendium came from UNDP's work in support of legal identity[2] systems (where identity management systems such as national ID card programmes can be the source of major privacy invasions if not implemented in comprehensive data protection and privacy legislative and institutional environments), all of UNDP's governance, human rights and digital transformation work can benefit from locating the UN's data protection and privacy texts in one place, which allows UNDP to be cognizant of these crucial policy areas in both their normative and advisory guises.

The research is divided into seven parts. Chapter 2 comprises the data protection and privacy-related normative frameworks as approved by Member State organs of the UN system. The third Chapter encompasses reports and other texts of the UN Special Rapporteurs, and the fourth Chapter addresses other non-normative inter-agency UN data protection and privacy-related activities. The fifth Chapter concentrates on data protection and privacy guidance within the UN departments, missions, commissions

[1] This report was drafted in 2021 by Anna Chenel under the guidance of the UNDP Bureau for Policy and Programme Support Governance Team's legal identity personnel, niall.mccann@undp.org and risa.arai@undp.org.

[2] The United Nations Economic and Social Council, approved the operational United Nations definition of **legal identity** in 2020, which is established of the "*basic characteristics of an individual's identity, name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally recognized identification authority. Legal identity should be linked to the civil registration system to ensure a holistic approach to legal identity from birth to death. Legal identity is retired by the issuance of a death certificate by the civil registration authority upon registration of death*. https://unstats.un.org/unsd/statcom/51st-session/documents/2020-15-CRVS-E.pdf

and agencies, funds and programmes (e.g., ILO, UNDP, WHO), as well as the World Bank. The sixth Chapter concerns selected data protection and privacy instruments outside of the UN system.

At the end, a comparison of selected data protection principles of this research is presented to attempt to identify which principles are common across the UN and the external organisations (and which can be considered of particular importance for legal identity systems).

1.2 Definitions

The term **privacy** is most used in the United States, while Europeans tend to speak more about **data protection**. For example, the 2018 *California Consumer Privacy Act*[3] applies in relation to personal information that businesses collect from consumers.[4] The European Commission Directive 95/46/EC of 24 October 1995, now repealed, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, however, was called the *Data Protection Directive*.

Daniel J. Solove ('Conceptualising Privacy', 2005) considers that privacy invasions disrupt and sometimes even completely annihilate certain practices, such as interference with peace of mind and tranquility, invasion of solitude, breach of confidentiality, threats to or violations of personal security, destruction of reputation, surveillance, and so on.[5] He lists information control as an important dimension of privacy in addition to the right to be left alone, limited access to the self, secrecy, personhood and intimacy. According to Solove, the matters we consider to be private are shaped by culture and history and have differed across cultures and historical epochs. The family, body, and home are aspects of life that are commonly viewed as private, even though they have not always been perceived as such.[6] Thinking in this way, 'data privacy' or 'data protection' could be considered as a part of the concept of privacy.

Personal data is defined in Article 4 of the European Union's General Data Protection Regulation as any information relating to an identified or identifiable natural person, and an "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[7] The term **personal information** is used to describe the same.

[3] 1798.100 - 1798.199.100.
[4] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
[5] Solove 2005, p. 1130
[6] Solove 2005, p. 1132-1138.
[7] 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 https://eur-lex.europa.eu/eli/reg/2016/679/oj

2. DATA PROTECTION AND PRIVACY-RELATED NORMATIVE FRAMEWORK AS APPROVED BY MEMBER STATE ORGANS OF THE UN SYSTEM

2.1 Key human rights instruments

2.1.1 Universal Declaration on Human Rights

Human rights are universal, inalienable, indivisible, and interdependent. Article 12 of the Universal Declaration of Human Rights (UDHR), proclaimed by the United Nations General Assembly in 1948, states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of law against such interference or attacks."[8]

When the right to privacy was recognized as an international human right in the UDHR, it had not been included in any state constitution. In the years after World War II, state constitutions protected only aspects of privacy, such as the inviolability of the home and of correspondence and unreasonable searches of the body. Such an umbrella "privacy" term was new, and the UDHR drafters were likely not aware that the term would open the door for the protection of further aspects of privacy not mentioned, nor even imagined at the time, in the codification process.[9]

The UDHR was an important reference for the European Convention of Human Rights, drafting of which commenced in August 1949 within the framework of the Council of Europe, roughly half a year after the adoption of the UDHR by the UN General Assembly.[10]

The UDHR was originally formulated as soft law, being aspirational and not legally binding. Its lack of legal status, however, has not prevented its significant influence in formulating legislation worldwide. It formed the basis for two covenants which have binding status in international law: the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), both of which were adopted by the General Assembly in 1966.[11]

2.1.2 International Covenant on Civil and Political Rights

The ICCPR came into force in March 1976. States that ratify it are legally bound by it, and therefore civil and political rights are directly applicable and judicially enforceable. As of today, 173 Member States have ratified the ICCPR.[12]

The provision on privacy in the ICCPR is worded almost identical to Article 12 of the UDHR, the sole difference being Article 17 of the ICCPR, which not only prohibits 'arbitrary' interference with one's privacy (and with more specific aspects of the private sphere), but also 'unlawful' ones:

[8] https://www.un.org/en/universal-declaration-human-rights/
[9] How the Right to Privacy Became a Human Right, p. 441.
[10] How the Right to Privacy Became a Human Right, p. 452.
[11] The ICESCR does not include any privacy provisions.
[12] https://indicators.ohchr.org/

- "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.
- Everyone has the right to the protection of the law against such interference or attacks."[13]

Other UN-level human rights texts that address data protection and privacy include Article 16 of the Convention on the Rights of the Child, Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, and Article 22 of the Convention on the Rights of Persons with Disabilities.

2.2 Reports of the High Commissioner for Human Rights and the Secretary-General, and Related Resolutions of the General Assembly and the Human Rights Council

2.2.1 General Assembly Resolution 45/95 on Guidelines for the Regulation of Computerised Personal Data Files[14]

This 1990 Resolution was the first UN instrument to address personal data. In response to the need for specific rules governing the collection and use of personal data or personal information, a new concept of privacy emerged, known in some jurisdictions as 'informational privacy' and in others as the 'right to informational self-determination'. This concept led to the development of special legal regulations that provide personal data protection. [15]

Part A of the 1990 Resolution contains the ten principles concerning the minimum guarantees that should be provided for in national law, and Part B relates to application of the Guidelines to personal data files kept by intergovernmental bodies. [16]

1. Principle of lawfulness and fairness	Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.
2. Principle of accuracy	Persons responsible for the compilation and keeping of files have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible, to avoid errors of omission. Files should be kept up to date regularly, or when the information contained in a file is used, as long as they are being processed.
3. Principle of purpose-specification	The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity, or be brought to the attention of the person concerned, to make it possible subsequently to ensure that: (a) All personal data collected and recorded remains relevant and adequate to the purposes so specified.

[13] https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[14] https://digitallibrary.un.org/record/105299?ln=en
[15] Handbook on European data protection law, 2018, p. 18.
[16] Guidelines for the Regulation of Computerized Personal Data Files, p.1. https://www.refworld.org/pdfid/3ddcafaac.pdf

	(b) None of said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified. (c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified.
4. Principle of interested-person access	Everyone who offers proof of identity has the right to know whether information concerning him or her is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary, or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if need be, with the supervisory authority specified in principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. The provisions of this principle should apply to everyone, irrespective of nationality or place of residence.
5. Principle of non-discrimination	Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, sex life, political opinions, religious, philosophical, and other beliefs as well as membership of an association or trade union, should not be compiled.
6. Power to make exceptions	Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause), provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards. Exceptions to principle 5 relating to the prohibition of discrimination, may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination.
7. Principle of security	Appropriate measures should be taken to protect the files against both natural dangers (e.g., accidental loss or destruction), and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by viruses.
8. Supervision and sanctions	The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles. This authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the principles, criminal or other penalties should be envisaged together with appropriate individual remedies.
9. Transborder data flows	When the legislation of two or more countries concerned by a trans-border data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.

10. Field of application	The present principles should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.

Part B of the Guidelines stated that a derogation from the principles may be specifically provided for when the purpose of the file is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance. Such a derogation should be provided in national legislation for governmental international organizations whose headquarters agreement does not preclude the implementation of the said national legislation as well as for non-governmental international organizations to which this law is applicable.[17]

2.2.2 General Assembly Resolution 68/167

No further major report or resolution on data protection or privacy was adopted by the Member State or human rights organs of the UN until the 2013 General Assembly Resolution 68/167, which called on all Member States to respect and protect the right to privacy, including in the context of digital communication, and to take legislative and other measures to put an end to violations of those rights, and to create the conditions to prevent such violations. States were also asked to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law. Independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data, were also asked to be established or maintained.[18]

The Resolution asked the High Commissioner for Human Rights to submit a report on the protection of the right to privacy in the context of domestic and extra-territorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council, with views and recommendations, for consideration by Member States.[19]

2.2.3 Report of the High Commissioner for Human Rights A/HRC/27/37

The subsequent June 2014 report of the High Commissioner for Human Rights concluded that practices in many Member States have revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.

[17] Guidelines for the Regulation of Computerized Personal Data Files, p.3.
[18] A/RES/68/167, p. 2-3. https://undocs.org/A/RES/68/167
[19] A/RES/68/167, p. 3. https://undocs.org/A/RES/68/167

The High Commissioner noted that courts at the national and regional levels are often engaged in examining the legality of electronic surveillance policies and measures. Surveillance policies and practices should be assessed against international human rights law, and a lack of governmental transparency associated with surveillance policies, laws and practices hinders any effort to assess their coherence with international human rights law and to ensure accountability. Effectively addressing the challenges related to the right to privacy in the context of modern communications technology will, according to the High Commissioner, require ongoing, concerted multi-stakeholder engagement. According to the report, States should review their own national laws, policies and practices to ensure full conformity with international human rights law, and, in particular, that effective and independent oversight regimes and practices are in place. [20]

2.2.4 Resolution A/HRC/RES/28/16 of the Human Rights Council

In response to the High Commissioner's report, the Human Rights Council, in its resolution in March 2015, decided to appoint, for a period of three years, a Special Rapporteur on the Right to Privacy. The tasks of the Special Rapporteur were to include:

- gathering relevant information, inter alia, on international and national frameworks, practices and experience; to study trends, developments and challenges in relation to the right to privacy, and; to make recommendations to ensure its promotion and protection in connection with the challenges arising from new technologies;
- seeking, receiving and responding to information, from Member States, the United Nations and its agencies, programmes and funds, regional human rights mechanisms, national human rights institutions, civil society organizations, the private sector, including business enterprises, and any other relevant stakeholders or parties;
- identifying possible obstacles to the promotion and protection of the right to privacy; to identify, exchange and promote principles and best practices at the national, regional and international levels; and to submit proposals and recommendations to the Human Rights Council in that regard, including with a view to particular challenges arising in the digital age;
- participating in and contributing to relevant international conferences and events with the aim of promoting a systematic and coherent approach on issues pertaining to the mandate;
- raising awareness concerning the importance of promoting and protecting the right to privacy, including with a view to particular challenges arising in the digital age, as well as concerning the importance of providing individuals whose right to privacy has been violated with access to effective remedy, consistent with international human rights obligations;
- integrating a gender perspective throughout the work of the mandate;
- reporting on alleged violations of the right to privacy, as set out in article 12 of the UDHR and article 17 of the ICCPR, including in connection with the challenges arising from new technologies, and drawing the attention of the Council and the United Nations High Commissioner for Human Rights to situations of particularly serious concern;

[20] A/HRC/27/37, p. 16. https://undocs.org/A/HRC/27/37

- submitting an annual report to the Human Rights Council and to the General Assembly, starting at the thirty-first session and the seventy-first session respectively.[21]

2.2.5 General Assembly Resolution 71/199

General Assembly Resolution 71/199 of 25 January 2017 made a call to business enterprises to meet their responsibility to respect human rights in accordance with the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, including the right to privacy in the digital age. Businesses were requested to inform users about the collection, use, sharing and retention of their data that may affect their right to privacy and to establish transparency policies, as appropriate. Finally, business enterprises were encouraged to work towards enabling secure communications and the protection of individual users against arbitrary or unlawful interference with their privacy, including by developing technical solutions. [22]

The Resolution encouraged all relevant stakeholders to participate in informal dialogues about the right to privacy and welcomed the contribution of the Special Rapporteur on the Right to Privacy in this process. The Human Rights Council was encouraged to remain actively seized of the debate, with the purpose of identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy, and to consider holding an expert workshop as a contribution for a future report of the United Nations High Commissioner for Human Rights on this matter.[23]

2.2.6 Resolution A/HRC/RES/34/7 of the Human Rights Council

In a further Resolution of the Council (March 2017), the High Commissioner was requested to organize an expert workshop with the purpose of identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age, including the responsibility of business enterprises in this regard, to prepare a report and to submit it to the Council.[24]

2.2.7 Report of the High Commissioner for Human Rights A/HRC/39/29

According to that report, submitted to the Council by the High Commissioner in August 2018, the need to address the challenges that the digital world brings to the right to privacy is more acute than ever. Driven mostly by the private sector, digital technologies that continually exploit data linked to people's lives, are progressively penetrating the social, cultural, economic and political fabric of modern societies. Increasingly powerful data-intensive technologies, such as big data and artificial intelligence, threaten to create an intrusive digital environment in which both States and business enterprises can conduct surveillance, analyse, predict and even manipulate people's behaviour to an unprecedented degree.[25] These data-intensive technologies present significant risks for human dignity, autonomy and privacy and the exercise of human rights in general, if not managed with great care.

---

[21] A/HRC/RES/28/16, p. 4-5. https://undocs.org/A/HRC/RES/28/16

[22] A/RES/71/199, p. 5-6. https://undocs.org/A/RES/71/199

[23] A/RES/71/199, p. 5-6. https://undocs.org/A/RES/71/199

[24] A/HRC/RES/34/7, p. 5. https://undocs.org/A/HRC/RES/34/7

[25] The Right to Privacy in the Digital Age, p. 2. https://undocs.org/A/HRC/39/29

The report refers to numerous international instruments and guidelines outside of the UN arena, forming a growing global consensus on minimum necessary standards to govern the processing of personal data by states, business enterprises and other private actors, namely: [26]

- The Convention for the Protection of Individuals about Automatic Processing of Personal Data of the Council of Europe;[27]
- The OECD Privacy Framework;[28]
- The African Union Convention on Cyber Security and Personal Data Protection;[29]
- The Madrid resolution on International Standards on the Protection of Personal Data and Privacy, and;[30]
- The Asia-Pacific Economic Coordination Privacy Framework.[31]

The Report discusses the different privacy interferences, responsibilities of states and business enterprises and remedies, and recommends the minimum standards for the processing of personal data. To conclude, the High Commissioner recommends States to:[32]

- Recognize the full implications of new technologies, in particular data-driven technologies, for the right to privacy, but also for all other human rights;
- Adopt strong, robust and comprehensive privacy legislation, including on data privacy, that complies with international human rights law in terms of safeguards, oversight and remedies to effectively protect the right to privacy;
- Ensure that data-intensive systems, including those involving the collection and retention of biometric data, are only deployed when Member States can demonstrate that they are necessary and proportionate to achieve a legitimate aim;
- Establish independent authorities with powers to monitor state and private sector data privacy practices, investigate abuses, receive complaints from individuals and organizations, and issue fines and other effective penalties for the unlawful processing of personal data by private and public bodies;
- Ensure, through appropriate legislation and other means, that any interference with the right to privacy, including by communications surveillance and intelligence-sharing, complies with international human rights law, including the principles of legality, legitimate aim, necessity and proportionality, regardless of the nationality or location of the individuals affected, and clarify that authorization of surveillance measures requires reasonable suspicion that a particular individual has committed or is committing a criminal offence or is engaged in acts amounting to a specific threat to national security;

[26] The Right to Privacy in the Digital Age, p. 9. https://undocs.org/A/HRC/39/29
[27] ETS No. 108 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
[28] http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[29] https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
[30] http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madrid_en.pdf
[31] https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)
[32] The Right to Privacy in the Digital Age, p. 16. https://undocs.org/A/HRC/39/29

- Ensure that the mechanisms required for State surveillance are competent and adequately resourced to monitor and enforce the legality, necessity and proportionality of surveillance measures;
- Review laws to ensure that they do not impose requirements of blanket, indiscriminate retention of communications data on telecommunications and other companies;
- Take steps to enhance transparency and accountability in the acquisition of surveillance technologies by States;
- Fully implement their duty to protect against abuses of the right to privacy by business enterprises in all relevant sectors, including the ICT sector, by taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication;
- Ensure that all victims of violations and abuses of the right to privacy have access to effective remedies, including in cross-border cases.

The High-Commissioner recommends business enterprises to: [33]

- Make all efforts to meet their responsibility to respect the right to privacy and all other human rights. At a minimum, business enterprises should fully operationalize the Guiding Principles on Business and Human Rights, which implies conducting effective human rights due diligence across their operations and in relation to all human rights, including the right to privacy, and taking appropriate action to prevent, mitigate and address actual and potential impacts;
- Seek to ensure a high level of security and confidentiality of any communications they transmit and personal data they collect, store or otherwise process. Conduct assessments on how best to design and update the security of products and services on an ongoing basis;
- Comply with the key privacy principles referred to in paragraphs 29–31 of the report and ensure the greatest possible transparency in their internal policies and practices that implicate the right to privacy of their users and customers;
- Cooperate in remediation through legitimate processes where they have caused or contributed to adverse impacts, including through effective operational-level grievance mechanisms;
- Contribute to the work of the OHCHR accountability and remedy project on developing guidance and recommendations to enhance the effectiveness of non-State-based grievance mechanisms in relation to abuses of the right to privacy in the digital space.

2.2.8 General Assembly Resolution 73/179

Resolution 73/179 of December 2018, drafted in consultation with all relevant stakeholders, including civil society, called upon the States to consider developing or maintaining and implementing adequate legislation, with effective sanctions and appropriate remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary processing of personal data by individuals, governments, business enterprises and private organizations. Promoting quality education and lifelong educational opportunities to foster, inter alia, digital literacy and

[33] The Right to Privacy in the Digital Age, p. 16-17.

technical skills to effectively protect privacy was also considered important in the Resolution. In addition, the Resolution stated that Member States should consider developing or maintaining legislation, preventive measures and remedies addressing harm from the processing, use, sale or multiple resale or other corporate sharing of personal data without the individual's free, explicit and informed consent. [34]

Business enterprises were called upon to inform users in a clear and easily accessible way about the collection, use, sharing and retention of their data that may affect their right to privacy and to establish transparency policies, as appropriate, as well as to implement administrative, technical and physical safeguards to ensure that data are processed lawfully, and to ensure that such processing is limited to what is necessary in relation to the purposes of the processing and its legitimacy. [35]

The Resolution called upon all States to further develop or maintain preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular effects on women, as well as children and those who are vulnerable and marginalized, and to consider developing, reviewing, implementing and strengthening gender-responsive policies that promote and protect the right of all individuals to privacy in the digital age. Business enterprises were encouraged to work towards enabling secure communications and the protection of individual users against arbitrary or unlawful interference with their privacy, including by developing technical solutions.[36]

2.2.9 Resolution A/HRC/RES/42/15 of the Human Rights Council

In September 2019, the Human Rights Council requested that Member States ensure that any measures taken to counter terrorism and violent extremism conducive to terrorism that interfere with the right to privacy are consistent with the principles of legality, necessity and proportionality, and comply with their obligations under international law. The High Commissioner for Human Rights was requested to organize a one-day expert seminar to discuss how artificial intelligence, including profiling, automated decision making, and machine-learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy, and to prepare a thematic report on the issue. States and business enterprises were called to take several actions in relation to the protection of the right to privacy.[37]

2.2.10 Report A/HRC/43/29 of the Secretary-General

The Secretary-General's report of 4 March 2020 was submitted pursuant to Human Rights Council resolution 40/12, in which the Council requested the Secretary-General to prepare an annual report on the question of the realization in all countries of economic, social and cultural rights, with a special focus on the role of new technologies for the realization of economic, social and cultural rights. The report identifies several actions that Member States and other stakeholders can take to harness the

[34] A/RES/73/179, p. 5-6. https://undocs.org/A/RES/73/179
[35] A/RES/73/179, p. 6. https://undocs.org/A/RES/73/179
[36] A/RES/73/179, p. 6-7.
[37] A/HRC/RES/42/15, p. 4-6. https://undocs.org/A/HRC/RES/42/15

opportunities of new technologies for the realization of economic, social and cultural rights, while addressing potential risks. [38]

The report states that many new technologies that hold promise in terms of promoting human well-being rely heavily on the processing of large amounts of personal data and that in such an environment, ensuring an adequate level of data privacy is essential to prevent human rights violations and abuses, including economic, social and cultural rights.[39]

The private sector should have responsibilities in the context of new technologies, according to the report, as their impact on economic, social and cultural rights can be particularly valuable to assess and address the risks of business models that involve, for example the following:

- collecting large volumes of personal health data and using and sharing such data without consent;
- using new technologies for public service delivery, in partnership with or on behalf of Governments, that could disproportionately put vulnerable populations at risks, and;
- providing and using technologies and technology-driven processes such as algorithms that may result in harm to people and direct and indirect discrimination.

The report refers to the Guiding Principles on Business and Human Rights (A/HRC/17/31), which recommend companies to carry out human rights due diligence across their activities and business relationships and states that human rights due diligence requirement extends across a company's operations, products and services, and applies to those related to the delivery of public services and goods, including in the areas critical for the realization of economic, social and cultural rights such as smart cities, health and education services. The report states that human rights due diligence should be embedded in company operations as an ongoing process, also integrating rights holder perspectives and experiences and that if new digital technologies are to fulfil their potential while mitigating accompanying risks, companies should meaningfully engage civil society, rights holders and vulnerable populations in their due diligence.[40]

To conclude, the Secretary-General recommends States, private companies and other stakeholders to:

- fully recognize the need to protect and reinforce all human rights in the development, use and governance of new technologies as their central objective, and ensure equal respect for and enforcement of all human rights online and offline;
- reaffirm and fulfil the obligations of States to adopt legislative measures, including measures concerning private sector activities, so that new technologies contribute to the full enjoyment of human rights by all, including economic, social and cultural rights, and adverse impacts on human rights are prevented, and;

[38] A/HRC/43/29, p. 1. https://undocs.org/A/HRC/43/29

[39] A/HRC/43/29, p. 13.

[40] A/HRC/43/29, p. 14.

- accelerate efforts to bridge digital divides and technological gaps between and within countries, and promote an inclusive approach to improving accessibility, availability, affordability, adaptability and quality of new technologies.[41]

2.2.11 Report A/HRC/44/24 of the High Commissioner for Human Rights

In the subsequent report of 24 June 2020, the High Commissioner recommends States to ensure that any interference with the right to privacy, including by communications surveillance and intelligence-sharing, complies with international human rights law, including the principles of legality, necessity and proportionality. Regarding facial recognition technology (in the context of peaceful assembly), the High Commissioner recommended Member States to:

- Systematically conduct human rights due diligence before deploying facial recognition technology devices, and throughout the entire life cycle of the tools deployed;
- Establish effective, independent and impartial oversight mechanisms for the use of facial recognition technology, such as independent data protection authorities, and consider imposing a requirement of prior authorization by an independent body for the use of facial recognition technologies in the context of peaceful assembly;
- Put in place strict privacy and data protection laws that regulate the collection, retention, analysis and otherwise processing of personal data, including facial templates;
- Ensure transparency about the use of image recordings and facial recognition technology in the context of assemblies, including through informed consultations with the public, experts and civil society, and the provision of information regarding the acquisition of facial recognition technology, the suppliers of such technology and the accuracy of the tools;
- When relying on private companies to procure or deploy these facial recognition technologies, request that companies carry out human rights due diligence to identify, prevent, mitigate and address potential and actual adverse impact on human rights and, in particular, ensure that data protection and nondiscrimination requirements be included in the design and the implementation of these technologies.[42]

2.2.12 General Assembly Resolution 75/176

Resolution 75/176 of December 2020 called upon all States to take appropriate measures to ensure that digital or biometric identity programmes are designed, implemented and operated with appropriate legal and technical safeguards in place, and in full compliance with the obligations of States under international human rights law.[43]

Business enterprises were encouraged to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption, pseudonymization and anonymity, and States were called upon not to interfere with the use of such

[41] A/HRC/43/29, p. 14-15. https://undocs.org/A/HRC/43/29

[42] A/HRC/ 44/24, p. 15-16. https://undocs.org/A/HRC/44/24

[43] A/RES/75/176, p. 7. https://undocs.org/en/A/RES/75/176

technical solutions, with any restrictions thereon complying with the obligations of States under international human rights law, and to enact policies that recognize and protect the privacy of individuals' digital communications. The contribution of the Special Rapporteur on the Right to Privacy was considered with appreciation, and the consideration of the question of right to privacy was decided to be continued at the following General Assembly session.

2.2.13 Report of the High Commissioner for Human Rights A/HRC/48/31

In September 2021, the High Commissioner for Human Rights issued a report to the Human Rights Council on some of the negative effects in the use of artificial intelligence, with privacy violation concerns to the fore, including his concerns on the use of invasive biometric technology, such as facial recognition, in public for as part of a State's internal security response.[44] Some of his recommendations specifically focused on privacy, including recommendations that member States:

> (a) Fully recognize the need to protect and reinforce all human rights in the development, use and governance of AI as a central objective…;
>
> (b) Ensure that the use of AI is in compliance with all human rights and that any interference with the right to privacy and other human rights through the use of AI is provided for by law, pursues a legitimate aim, complies with the principles of necessity and proportionality and does not impair the essence of the rights in question;
>
> (c) Expressly ban AI applications that cannot be operated in compliance with international human rights law and impose moratoriums on the sale and use of AI systems that carry a high risk for the enjoyment of human rights, unless and until adequate safeguards to protect human rights are in place;
>
> (d) Impose a moratorium on the use of remote biometric recognition technologies in public spaces, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards;
>
> (e) Adopt and…enforce, through independent, impartial authorities, data privacy legislation for the public and private sectors as an essential prerequisite for the protection of the right to privacy in the AI context;
>
> (f) Adopt legislative and regulatory frameworks that adequately prevent and mitigate the multifaceted adverse human rights impacts linked to the use of AI by the public and private sectors;
>
> (i) Enhance efforts to combat discrimination linked to the use of AI systems by States and business enterprises, including by conducting, requiring and supporting systematic assessments and monitoring of the outputs of AI systems and the impacts of their deployment;
>
> (j) Ensure that public-private partnerships in the provision and use of AI technologies are transparent and subject to independent human rights oversight...

The High Commissioner also recommended that Member States and businesses:

[44] https://undocs.org/A/HRC/48/31

(a) Systematically conduct human rights due diligence and human rights impact assessment throughout the life cycle of AI systems;

(b) Dramatically increase the transparency of their use of AI, including by adequately informing the public and affected individuals and enabling independent and external auditing of automated systems...;

(d) Advance the explainability of AI-based decisions, including by funding and conducting research towards that goal.

The High Commissioner specifically recommended, among others, that businesses:

(a) Make all efforts to meet their responsibility to respect all human rights, including through the full operationalization of the Guiding Principles on Business and Human Rights;

(b) Enhance their efforts to combat discrimination linked to their development, sale or operation of AI systems;

(c) Take decisive steps in order to ensure the diversity of the workforce responsible for the development of AI;

(d) Provide for or cooperate in remediation through legitimate processes where they have caused or contributed to adverse human rights impacts, including through effective operational-level grievance mechanisms.

2.3 UN Counter-Terrorism Instruments and Their Privacy Implications

2.3.1 International Convention for the Suppression of the Financing of Terrorism

The 199 International Convention for the Suppression of the Financing of Terrorism, which entered into force in April 2002, was adopted by the General Assembly in Resolution 54/109. The Convention criminalizes financing acts of terrorism, while promoting police and judicial cooperation and exchange of personal information to prevent, investigate and punish the financing of such acts. However, the Convention does not include any provisions relating to the protection of personal data.[45]

2.3.2 Security Council Resolution 1373

The September 2001 Security Council Resolution 1373 on Threats to International Peace and Security caused by terrorist acts reaffirmed its unequivocal condemnation of the terrorist attacks which took place on 11 September 2001 and expressed its determination to prevent all such acts with the decision. The Resolution is not a data protection instrument, but it encourages Member States to exchange information especially regarding action or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups. Member States are to exchange information in accordance with

[45] https://www.un.org/law/cod/finterr.htm

international and domestic law and to cooperate on administrative and judicial matters to prevent the commission of terrorist acts.[46]

2.3.3 Security Council Resolution 2160

Adopted in 2014, Security Council Resolution 2160 was the first thematic counter-terrorism resolution to explicitly highlight the exchange of biometric data as an important counter-terrorism tool. More precisely, the Security Council encouraged Member States, in accordance with their national legislation, to submit to INTERPOL, where available, photographs and other biometric data of individuals for the inclusion in the INTERPOL United Nations Security Council Special Notices.[47]

2.3.4 Security Council Resolution 2322

Resolution 2322 (2016) was the first Security Council instrument to focus specifically on international law enforcement and judicial cooperation in countering terrorism. The Security Council called upon States to share, where appropriate, information about foreign terrorist fighters and other individual terrorists and terrorist organizations, including biometric and biographic information, as well as information that demonstrates the nature of an individual's association with terrorism via bilateral, regional and global law enforcement channels.[48]

2.3.5 Security Council Guiding Principles on Foreign Terrorist Fighters

Security Council Resolution 2178 (2014) acknowledged the increasing threat posed by foreign terrorist fighters and required Member States to prevent and suppress, consistent with their obligations under international human rights law, international refugee law and international humanitarian law, the recruiting, organizing, transporting or equipping of foreign terrorist fighters, stop individuals believed to be foreign terrorist fighters from entering or transiting through their territory, and ensure that their domestic laws and regulations establish serious criminal offences enabling them to prosecute and penalize prohibited conduct related to foreign terrorist fighters.[49]

The Security Council Guiding Principles on Foreign Terrorist Fighters are composed of the 2015 Madrid Guiding Principles and the 2018 Addendum. The December 2018 Addendum (S/2018/1177) includes several privacy-relevant principles, including:

- Improving capabilities for detecting and interdicting terrorist travel, including effective use of advance passenger information and passenger name record data (principle 36);
- Developing watch lists and databases and sharing information through bilateral and multilateral mechanisms (principle 37);
- Developing biometric systems and ensuring their responsible use (principle 38).

The importance of the respect of international human rights law, including freedom of expression and right to privacy, is recalled several times in the Guiding Principles. The document states that any

[46] https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf
[47] https://www.undocs.org/S/RES/2160%20(2014)
[48] https://undocs.org/S/RES/2322(2016)
[49] Security Council Guiding Principles on Foreign Terrorist Fighters, p. 1. https://www.un.org/sc/ctc/wp-content/uploads/2019/09/Security-Council-Guiding-Principles-on-Foreign-Terrorist-Fighters.pdf

restrictions on privacy shall only be permitted when provided by law and are necessary on the grounds set out in paragraph 3 of article 19 of the ICCPR, and should not be subjected to arbitrary or unlawful interference with privacy, when:

- Collecting evidence through ICT and social media that can be admitted as evidence in cases related to foreign terrorist fighters;[50]
- Using passenger name record systems and advance passenger information;[51]
- Processing passenger name record data and considering retention frameworks;[52]
- Using biometric systems for the identification of terrorist suspects.[53]

2.3.6 UN Security Council Resolution 2396 (2017)

The December 2017 UNSC Resolution 2396 states that Member States shall develop the capability to collect, process and analyze, in furtherance of International Civil Aviation Organization (ICAO) standards and recommended practices on passenger name record (PNR) data, and urges ICAO to work with its Member States to establish a standard for the collection, use, processing and protection of PNR data.[54]

Additionally, the Resolution states that Member States shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, to identify terrorists responsibly and properly, including foreign terrorist fighters, in compliance with domestic law and international human rights law. It also encourages Member States to share this data responsibly among relevant Member States and with INTERPOL and other relevant international bodies.[55]

2.3.7 UN Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counterterrorism[56]

In order to assist Member States to use biometric technology in a responsible manner for counter-terrorism purpose, the UN Counter-Terrorism Executive Directorate (UNCTED) and the United Nations Office of Counter-Terrorism (UNOCT), at its Counter-Terrorism Centre (UNCCT), in partnership with the Biometrics Institute (UK), developed the Compendium of Recommended Practices for the responsible use and sharing of biometrics in counter-terrorism, in 2018, which provides a high-level overview of biometric technology, operating systems within the context of counter terrorism, but also information on the governance and regulatory requirements for biometric technology from the perspectives of

[50] Guiding Principle 25.
[51] Security Council Guiding Principles on Foreign Terrorist Fighters, p. 23.
[52] Guiding Principle 36.
[53] Security Council Guiding Principles on Foreign Terrorist Fighters, p. 27.
[54] Security Council Resolution 2396 (2017), p. 7. https://undocs.org/S/RES/2396(2017)
[55] Security Council Resolution 2396 (2017), p. 8. https://undocs.org/S/RES/2396(2017)
[56] https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_on_biometricsl_eng.pdf

international law, human rights law, ethical reviews, data protection requirements and the right to privacy.[57] The privacy-related information in it is also applicable to non-biometric personal data.

The Compendium noted that biometric technology can be a significant asset in countering terrorism on a global scale. However, the technology is based on the collection, storage and sharing of highly sensitive personal data and is therefore protected by law and must be processed without violating the right to privacy.

According to the Compendium, law enforcement authorities can limit the right to privacy if the measures taken are necessary and proportionate and in compliance with international human rights law. For example, personal data of suspects and associates may be used in emergencies, where key privacy principles such as informed consent or the harvesting of related personal data may be set aside. However, privacy principles such as informed consent, collection and use only for stated purposes, and the right to correct inaccurate or misleading records, should be treated as the default requirements in most cases. The sharing of personal data, including biometrics, must be lawfully approved domestically and subject to a clear legal framework between the entities sending and receiving data, domestically and internationally. Data can be shared only with trusted recipients and personal data should not be sent to jurisdictions where privacy protection levels are below that of the sending country. [58]

The Compendium states that an organization responsible for data processing must nominate a data controller who will be responsible for managing all data processing activities including the collection, storage, use and deletion of the data. The data controller retains responsibility, even if the data processing function is outsourced to other parties.[59]

Adverse legal consequences and other damage may be caused to individuals through the misuse of personal data, according to the Compendium. This applies particularly to Terrorist 'watch lists' or other alert mechanisms. Strong safeguards, including oversight mechanisms by an independent body, must be in place against the arbitrary collection, storage and use of personal data. States may already have privacy oversight bodies in place that could undertake this function as part of an existing or expanded remit. The Compendium states also that adequate remedies in law should be provided for breaches of privacy and other human rights in the handling of biometric data.[60]

2.3.8 Letter concerning counter-terrorism addressed to the President of the Security Council

A December 2019 letter from the Chair of the Security Council Committee, established pursuant to resolution 1373 (2001) concerning counterterrorism, was submitted to the Security Council to assist the Counter-Terrorism Committee Executive Directorate and Member States within the framework of

[57] United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter Terrorism, p. 4.
[58] Compendium, p. 31-33.
[59] Compendium, p. 32.
[60] Compendium, l. 35.

the country assessments prepared by the Directorate on behalf of the Committee.[61] The letter considers data protection and privacy in relation to the following matters:

- Suppressing and preventing recruitment: Does the implementation of the criminalization of recruitment and of the national strategy for the suppression of recruitment provide full respect for the rights of individuals, including the rights to freedom of association, freedom of expression, freedom of religion, and privacy?[62]
- Investigating, prosecuting and adjudicating terrorist acts: How does the State take into account the need to prevent arbitrary or unlawful interference with privacy?[63]
- Exchange of data: any infringement upon the right to privacy must comply with the principles of necessity and proportionality as well as non-discrimination;[64]
- Digital evidence: Does the State ensure respect for the data subjects' right to freedom from arbitrary or unlawful interference with privacy under international law, as well as for relevant protections under national law, which may include access, rectification, restrictions on use and judicial redress? [65]
- Digital evidence: Has the State put in place sufficient governance mechanisms, regulations, data protection, privacy policies, risk management and vulnerability assessments to collect, process and use forensic evidence, including biometrics, responsibly and properly and in full compliance with international human rights obligations? [66]
- Rights of victims in criminal proceedings: Does the State have adequate safeguards and security measures in place to ensure the protection of victims' rights to life, physical security and privacy?[67]
- Effective border security: Does the State have the necessary safeguards in place to ensure that information contained in watch lists and no-fly lists is not misused in a manner that threatens human rights and is maintained with full respect for the right to privacy? [68]
- Effective use of advance passenger information and passenger name records: Do passenger name record data-processing and retention frameworks incorporate oversight and privacy protections? Are precautions taken against the misuse or abuse of the data by State authorities?[69]

[61] Letter dated 27 December 2019 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counterterrorism addressed to the President of the Security Council, p. 1. https://www.undocs.org/en/S/2019/998
[62] Letter, p. 37.
[63] Letter, p. 61.
[64] Letter, p. 64.
[65] Letter, p. 65.
[66] Letter, p. 68.
[67] Letter, p. 77.
[68] Letter, p. 98.
[69] Letter, p. 107.

- Exchanging information: Safeguards linked to the right to privacy and presumption of innocence, as well as practices that collect, store and share information in a non-discriminatory manner consistent with international human rights law. [70]

3 REPORTS AND OTHER TEXTS OF THE UN SPECIAL RAPPORTEURS

3.1 Report A/72/540 of the Special Rapporteur on Privacy

The October 2017 report of the Special Rapporteur on Privacy includes an overview of activities of the Special Rapporteur in 2016 –2017 and an interim report of Task Force on Big Data and Open Data, established by the SR. The SR considers that data is and will remain a key economic asset, like capital and labour, and that understanding how to use big data efficiently – and how to share its benefits fairly without eroding the protection of human rights – will be hard, but ultimately worthwhile. The SR opined that any open government initiative involving personal information, whether de-identified or not, requires a rigorous, public, scientific analysis of data privacy protections, including a privacy impact assessment. [71]

To conclude, the SR makes the following statements:

- Open data policies require clear statements on the limits to the use of personal information, based on international standards and principles, including an exempt category for personal information with a binding requirement to ensure the reliability of de-identification processes to render this information appropriate for release as open data, and robust enforcement mechanisms.
- Any open government initiative involving personal information, whether de-identified or not, requires a rigorous, public, scientific analysis of data privacy protections, including a privacy impact assessment.
- Sensitive high-dimensional unit-record level data about individuals should not be published online or exchanged unless there is sound evidence that secure de-identification has occurred and will be robust against future re-identification.
- Frameworks should be established to manage the risk of sensitive data being made available to researchers.
- Governments and corporations should actively support the creation and use of privacy-enhancing technologies.

The SR's recommendations regarding big data include the following topics: governance, regulatory environment, inclusion of feedback mechanisms and research. He considers that in research relatively new techniques such as differential privacy and homomorphic encryption should be investigated to assess if they provide adequate privacy processes and outputs. He also recommends investigating citizens' awareness of the data activities of governments and businesses, the uses of personal

[70] Letter, p. 121.
[71] Report A/72/540, p. 24. https://undocs.org/pdf?symbol=en/A/72/540

information, including for research, and technological mechanisms to enhance individual control of their data and to increase their ability to utilize it for their needs. [72]

3.2 Draft text for a proposed Legal Instrument on Government-led Surveillance and Privacy

The January 2018 text of the SR states that there is significant concern that states cannot move in a rights-positive direction on surveillance, and that a legal instrument could be an opportunity for 'regressive negotiation'. The terms and concepts used in this text depend on effectively working state institutions, operating based on the rule of law and ultimately drawing from a culture that is fully committed to respecting, protecting and promoting human rights. Surveillance needs to be limited to what is necessary and proportionate, while states need to be able to guarantee a safe and secure environment. Questionable and bad practices ultimately weaken human rights, the national and international legal order and result in a situation which threatens to lower human dignity and cause physical harm to persons all over the world. Even though the SR did not necessarily agree with all parts of the text which were included he presented them in the spirit of open discussion. [73]

3.3 Recommendation on the protection and use of health-related data

The Recommendation on the protection and use of health-related data of December 2019 was prepared in the framework of the Task Force on Privacy and the Protection of Health-Related Data, established by the SR. The recommendation provides guiding principles concerning data processing of health-related data and emphasizes the importance of a legitimate basis of data processing of health-related data by all sectors of society, including public authorities and commercial organizations.

The Recommendation serves as a common international baseline for minimum data protection standards for health-related data for implementation at the domestic level and is a reference point for the ongoing debate on how the right to privacy can be protected in the context of health-related data, in conjunction with other human rights, where health-related data is processed and shared globally. The Recommendation applies to the data processing of health-related data in all sectors of society including the public and private sectors, not limiting or otherwise affecting any law, however, that grants data subjects more, wider or better rights, protection, and/or remedies than the Recommendation. [74]

Chapter II of the Recommendation includes Principles concerning data processing of health-related data as well as rules regarding lawful basis of data processing, notifiable diseases and health-related data, genetic data, sharing, disclosure and administering health care and storage of health-related data. [75] Chapter III includes recommendations regarding the rights of the data subject. Recommendations

[72] Report A/72/540, p. 24-25.
[73] Working Draft Legal Instrument on Government-led Surveillance and Privacy, p. 2. https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf
[74] Recommendation on the protection and use of health-related data, p. 3. https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf
[75] Recommendation on the protection and use of health-related data, p. 8-14, https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf

related to health-related data and indigenous data sovereignty, people living with disabilities, gender and other themes in relation with health-related data are provided.

3.4 Report A/HRC/43/52 of the Special Rapporteur on Privacy on Gender-Based Privacy Infringements

This March 2020 report was prepared pursuant to Human Rights Council resolution 28/16. The thematic focus of the report is reflected in recommendations for protecting against gender-based privacy infringements. The SR states that privacy and gender have long been regarded as second-order considerations, but their complex impact on society is of critical importance and that deeply disturbing infringements of privacy related to an individual's gender have arisen. Gender-based breaches of privacy are a systemic form of the denial of human rights, are discriminatory in nature and frequently perpetuate unequal social, economic, cultural and political structures.

Everyone, irrespective of their biological sex, sex characteristics, sexual orientation or gender identity or expression, is entitled to the full enjoyment of the right to privacy. In his report, the SR gives recommendations for protecting against gender-based privacy infringements that are intended to cover both state and non-state actors and are relevant to the privacy of all individuals, inclusive of binary female and male individuals and those of diverse sexual orientation, gender identity, gender expression and sex characteristics. The recommendations for protecting against gender-based infringements of privacy relate to themes such as:

- development of personality and the person (e.g., the right to gender identity privacy and the freedom of individuals to make autonomous decisions about their bodies);
- the privacy rights of indigenous people, persons with disabilities, children, young people and asylum seekers;
- work, social security protection, housing and education;
- security and surveillance;
- physical autonomy, reproductive rights and well-being and health care;
- digital technologies and online digital platforms.

On gender identity, legal recognition and the right to privacy, the SR's recommendations included that Member States should ensure that official identity documents include only relevant, reasonable and necessary personal information relating to sex and gender, as required by law for a legitimate purpose, and that clear and publicly accessible information is provided on how sex and gender information can be changed on personal records.

3.5 Draft Data Privacy Guidelines in context of Artificial Intelligence

The aim of the SR's Data Privacy Guidelines for the development and operation of Artificial Intelligence solutions is to provide guiding principles concerning the use of personal and personal related information in the context of artificial intelligence (AI) solutions, and to emphasise the importance of a legitimate basis for AI data processing by governments and corporations. The Guidelines are intended to serve as a common international minimum baseline for data protection standards regarding AI

solutions, especially those to be implemented at the domestic level, and to be a reference point for the ongoing debate on how the right to privacy can be protected in the context of AI solutions.[76]

They are applicable to the data processing of AI solutions in all sectors of society including the public and private sectors and to all controllers of AI solutions. 'Controller' in this context means designer, developer or operator (self-responsible or principal) each in its specific function. Data processing in this context means the design, the development, the operation and decommissioning of an AI solution. [77]

The Guidelines propose that irrespective of the jurisdiction or the legal environment applying to the controller, seven main principles are mandatory considerations in the planning and implementation of AI solutions:[78]

- **Jurisdiction**: To create legal certainty and traceability, AI solutions should be implemented and operated in a single jurisdiction, and that jurisdiction should have suitable legislation for best practice governance and risk management of the AI.
- **Lawful basis and purpose limitation**: As the processing of personal data of individuals always intrudes into the rights of the data subject, an AI solution must have a sound legal basis if it deals with personal data.
- **Accountability**: Each AI solution needs either a legal or a natural person that takes the full responsibility for the data processing and its results.
- **Control**: AI solutions must be under full control of the controller.
- **Transparency and explainability**: AI solutions must be made transparent to the public and the data subjects. The information must cover all relevant aspects that might be of interest regarding the evaluation of the solution and possible rights of the data subjects.
- **Rights of the "data subject"**: right to withdraw consent, to access, to object and other rights should be guaranteed for data subjects.
- **Safeguards**: AI solutions shall function in a robust way and shall be secured by appropriate safeguards against risk, using methods that foster trust and understanding across all parties involved, including the data subjects and the public.

3.6 Reports of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

In his 2013 report (A/HRC/23/40), the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression makes statements on communications surveillance measures. He considers that communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. The report states that the public should have increasing access to information, understanding and awareness of threats to privacy and the States should refrain from

[76] Draft Data Privacy Guidelines in context of Artificial Intelligence, p. 1.
https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2020_Sept_draft_data_Privacy_guidelines.pdf
[77] Draft Data Privacy Guidelines in context of Artificial Intelligence, p. 1-2.
[78]Draft Data Privacy Guidelines in context of Artificial Intelligence, p. 6-9.

forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption. In conclusion the Special Rapporteur states that human rights mechanisms should further assess the obligations of private actors developing and supplying surveillance technologies.[79]

In a later 2015 report (A/HRC/29/32), the Special Rapporteur concludes that encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. He recommends States to revise or establish national laws and regulations to promote and protect the rights to privacy and freedom of opinion and expression. With respect to encryption and anonymity, States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions that meet the requirements of legality, necessity, proportionality and legitimacy in objective, require court orders for any specific limitation, and promote security and privacy online through public education on a case-specific basis. He recommends that States, international organizations, corporations and civil society groups promote online security.[80]

[79] Report A/HRC/23/40, p. 20-23. https://undocs.org/A/HRC/23/40
[80] Report A/HRC/29/32, p. 20. https://undocs.org/A/HRC/29/32

4 OTHER NON-NORMATIVE INTER-AGENCY UN PRIVACY AND DATA PROTECTION-RELATED INITIATIVES

4.1 Global Working Group on Big Data for Official Statistics

In March 2014 the UN Statistical Commission established a Global Working Group on Big Data for Official Statistics ("GWG") to provide strategic vision, direction and coordination of a global programme on big data for official statistics.[81] The GWG is composed of 31 Member States and 16 international organizations.[82] Privacy issues, and in particular those relevant to the use and reuse of data, data linking, re-identification and cross-border data, are part of the mandate of the Global Working Group.

The GWG delivers most of its work through task teams, which develop methods, prepare handbooks, conduct capacity-building activities, acquire data, make algorithms available in the methods service and demonstrate the active use of the data and services available on the United Nations Global Platform.

In the framework of the GWG, one of the task teams created (in 2018) is on Privacy-Preserving Techniques (PPTTT). Promoting the use of privacy-preserving techniques was also on the agenda of the 6th International Conference on Big Data for Official Statistics in 2020. The PPTTT advises the GWG on developing the data policy framework for governance and information management of the global platform, specifically around supporting privacy preserving techniques developing and proposing principles, policies, and open standards for encryption within the UN Global Platform to cover the ethical use of data and the methods and procedures for the collection, processing, storage and presentation of data taking full account of data privacy, confidentiality and security issues.[83]

The PPTTT focuses on approaches to preserve privacy in the statistical analysis of sensitive data and presents examples of use cases where such methods may apply. The methods enable protection of the privacy of data while it is being processed rather than while it is at rest in a system or in transit between systems.[84]

As its first deliverable the task team published UN Handbook on Privacy Preserving Techniques ("Handbook"). The Handbook describes motivations for privacy-preserving approaches for the statistical analysis of sensitive data systems and is intended for use by statisticians and data scientists, data curators and architects, IT specialists, and security and information assurance specialists. Its focus is on methods that enable protecting privacy of data while it is being processed rather than while it is at rest on a system or in transit between systems.[85]

The Handbook explains that privacy threats and leakages may be intentional (a hacker, curious data analyst) or unintentional (unexpected sensitive result during the analysis). Privacy Enhancing Technologies can reduce the risks for both intentional and unintentional leakages. The Handbook states that it is important that Privacy Enhancing Technologies are applied by the data owner, on premises, and before releasing confidential data to third parties.[86] The Handbook presents several Privacy-Enhancing Technologies in the Handbook, including Secure Multiparty Computation (MPC),[87] (Fully)

Homomorphic Encryption (HE or FHE), [88] Differential Privacy,[89] Zero Knowledge Proofs (ZK Proofs)[90] and Trusted Execution Environments (TEE).[91]

Four existing standards and three, that are in development, are presented in the Handbook. ISO/IEC 29101:2013 (Information technology – Security techniques – Privacy architecture framework) is one of the oldest standards efforts that handles secure computing. It presents architectural views for information systems that process personal data and show how Privacy Enhancing Technologies such as secure computing, but also pseudonymisation, query restrictions and more could be deployed to protect Personally Identifiable Information.[92] In addition the Handbook gives information on legal research and trainings in Privacy Enhancing Technologies.[93]

4.2 UN Development Group – Guidance Note on Big Data for Achievement of the 2030 Agenda

The November 2017 Guidance Note on Big Data for Achievement of the 2030 Agenda, development of which was led by UN Global Pulse, was approved by the United Nations Development Group (UNDG)[94] and sets out general guidance on data privacy, data protection and data ethics for the UNDG concerning the use of big data, collected in real time by private sector entities as part of their business offerings. The Guidance Note recommends that more detailed operational guidelines should be created to implement the principles. It also recommends that designated legal, ethics, privacy and security experts should be consulted regarding the implementation of, and compliance with, the Guidance Note. A monitoring mechanism for compliance and implementation of the Note is encouraged to be implemented.[95] The Guidance Note is designed to: [96]

- establish common principles across UNDG to support the operational use of big data for achievement of the Sustainable Development Goals (SDGs);

[81] Terms of reference and mandate of the Global Working Group on Big Data for Official Statistics, p. 2. https://unstats.un.org/bigdata/documents/TOR%20-%20GWG%20-%202015.pdf
[82] https://unstats.un.org/bigdata/about/membership.cshtml#bureau
[83] UN Privacy Preserving Techniques Handbook, p. 3. http://publications.officialstatistics.org/handbooks/privacy-preserving-techniques-handbook/UN%20Handbook%20for%20Privacy-Preserving%20Techniques.pdf
[84] Report of the Global Working Group on Big Data for Official Statistics. E/CN.3/2021/14, p. 3-5.
[85] https://marketplace.officialstatistics.org/privacy-preserving-techniques-handbook
[86] Handbook, p. 13-14.
[87] Handbook, p. 20-25.
[88] Handbook, p. 25-27.
[89] Handbook, p. 31-36.
[90] Handbook, p. 36-39.
[91] Handbook, p. 41-45.
[92] Handbook, p. 45.
[93] Handbook, p. 48-50.
[94] Guidance Note, p. 2. https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf. The approval of the Guidance Note is based on consensus among UNDG members, and the provisions apply to all UNDG entities: FAO, IFAD, ILO, IOM, ITU, OHCHR, UNAIDS, UNCTAD, UNDESA, UNDP, UNECA, UNECE, UNECLAC, UNEP, UNESCAP, UNESCO, UNESCWA, UNICEF, UNIDO, UNFPA, UNHABITAT, UNHCR, UNODC, UN OHRLLS, UNOPS, UN OSAA, SRSG/CAC, UN Women, UNWTO, WFP, WHO and WMO
[95] Guidance Note, p.3.
[96] Guidance Note, p. 9.

- serve as a risk-management tool considering fundamental human rights, and;
- set principles for obtaining, retention, use and quality control for data from the private sector.

The Guidance Note recognizes, and is based on, the 1990 UN Guidelines for the Regulation of Computerized Personal Data Files and considers both existing international instruments and relevant regulations, rules and policies of UNDG member organizations concerning data privacy and data protection. The guidance is based on standards that have withstood the test of time, reflecting the strength of their core values. Its aim is to support members and partners of the UNDG in establishing efficient and coherent data collaborations and to provide a harmonized general framework for accountable, adequately transparent, and responsible data handling practices across the UNDG and with partners. It may be expanded and elaborated on by the implementing organizations.[97]

There are many definitions for 'big data' and many types of big data with potential utility for development according to the Guidance Note. UN Global Pulse defines big data as "a massive volume of both structured and unstructured data that is so large that it's difficult to process with traditional database and software techniques."[98]

The Guidance Note sets the following nine principles for personal data processing.

<table>
<tr><td rowspan="4">Lawful, legitimate and fair use</td><td>Data access, analysis or other use must be consistent with the United Nations Charter and in furtherance of the Sustainable Development Goals. The use of personal data should be based on one or more legitimate and fair bases.
Data should be obtained, collected, analysed or otherwise used through lawful, legitimate and fair means. In particular, data access (or collection, where applicable), analysis or other use should be in compliance with applicable laws, including data privacy and data protection laws, as well as the highest standards of confidentiality and moral and ethical conduct.</td></tr>
<tr><td>Big data often contains personal data and sensitive data. The use of personal data should be based on one or more of the following legitimate and fair bases, subject to implementing UNDG member organizations' regulations, rules and policies (including data privacy and data protection policies):</td></tr>
<tr><td>(i) adequate consent of the individual whose data is used,
(ii) in accordance with law,
(iii) furtherance of international organizational mandates,
(iv) other legitimate needs to protect the vital or best interest of an individual(s) or group(s) of individuals.</td></tr>
<tr><td>Purpose specification, use limitation and purpose compatibility</td><td>Any data use must be compatible or otherwise relevant, and not excessive in relation to the purposes for which it was obtained.</td></tr>
</table>

[97] Guidance Note, p. 2-3.
[98] Guidance Note, p. 9.

Risk mitigation and risks, harms and benefits assessment	A risks, harms and benefits assessment that accounts for data protection and data privacy (as well as ethics of data use) should be conducted before a new or substantially changed use of data (including its purpose) is undertaken. Also, the assessment should consider the digital literacy of both potential users of data and those individuals whose data is being used.
Sensitive data and sensitive contexts	This Principle proposes that stricter standards of data protection should be employed while obtaining, accessing, collecting, analysing or otherwise using data on vulnerable populations and persons at risk, children and young people, or any other sensitive data.[99]
Data security	Data security is crucial in ensuring data privacy and data protection.
	Proactively embedding the foundational principles of Privacy by Design and employing privacy enhancing technologies during every stage of the data life cycle is strongly recommended as a measure to ensure robust data protection. Personal data should be de-identified, where appropriate. Personal and sensitive data should be encrypted when transferred to or from any network-connected server.
Data retention and data minimization	Data access, analysis or other use should be kept to the minimum amount necessary to fulfill its purpose.
	The amount of data, including its granularity, should be limited to the minimum necessary. Data use should be monitored to ensure that it does not exceed the legitimate needs of its use. No extra or just-in-case data set is stored. The data should be permanently deleted upon conclusion of the time period needed to fulfill its purpose, unless its extended retention is justified. [100]
Data quality	All data-related activities should be designed, carried out, reported and documented with an adequate level of quality and transparency. Data should be validated for accuracy, relevancy, sufficiency, integrity, completeness, usability, validity and coherence, and be kept up to date.
	Automatic processing of data, including the use of algorithms, without human intervention and domain expertise should be avoided when data is analysed for decision-making that is likely to have any impact on an individual(s) or group(s) of individuals to avoid potential harms resulting from low quality of data.
	A periodic assessment of data quality is recommended during the data life cycle. Furthermore, it is important to establish an internal system of constant data updating and deletion of obsolete data, where appropriate and practically possible.[101]

[99] Guidance Note, p. 4-5.

[100] Guidance Note, p. 5-6.
[101] Guidance Note, p. 6-7.

Open data, transparency and accountability	Appropriate governance and accountability mechanisms should be established to monitor compliance with relevant law, including privacy laws and the highest standards of confidentiality, moral and ethical conduct with regard to data use.
Due Diligence for third party collaborators	Third party collaborators engaging in data use should act in compliance with relevant laws, including privacy laws as well as the highest standards of confidentiality and moral and ethical conduct.
	It is recommended that a process of due diligence be conducted to evaluate the data practices of any potential third-party collaborators.
	Legally binding agreements outlining parameters for data access and handling (e.g., data security, data formats, data transmission, fusion, analysis, validation, storage, retention, re-use, licensing, etc.) should be established to ensure reliable and secure access to data provided by third party collaborators. [102]

4.3 Expert Group on Governance of Data and Artificial Intelligence

The Data Privacy Advisory Group was established by UN Global Pulse in 2014 to address the challenges posed by the use and non-use of data for global development, peace and humanitarian action in response to the "data revolution." In 2019 the Group was expanded to incorporate greater expertise in AI ethics and human rights, given the rapid development and use of emerging technologies across all sectors globally. Members' expertise informs the development of strategies and guidelines on the ethical and privacy-protective use of data and AI, while preserving their transformative value for the achievement of the 2030 Agenda.

The Expert Group currently includes 33 international leaders from the public sector, civil society, private sector and legal community who serve as advocates for privacy and the human rights-centric approach to data and AI for purposes of sustainable development, humanitarian action and peace. Group members serve in their personal capacity, not as representatives of their affiliated organizations. Opinions and feedback gathered by the Expert Group are based on members' own field of expertise and generally accepted privacy principles and ethical standards.[103]

4.4 UN Privacy Policy Group

The UN Privacy Policy Group (UN PPG), established in 2016, is co-chaired by UN Global Pulse and the UN Office of Information and Communications Technology. The UN PPG meets several times a year and is comprised of privacy, information security and legal experts from over 30 UN entities. The UN Principles on Personal Data Protection and Privacy is one of the most significant contributions of the UN Privacy Policy Group. The primary objectives of UN PPG are to:

- Facilitate dialogue and knowledge sharing on data privacy and protection within the UN;
- Unite efforts on data privacy and data protection across the UN, and;

[102] Guidance Note, p. 7.
[103] https://www.unglobalpulse.org/policy/expert-group-on-governance-of-data-and-ai/

- Build capacity and ensure responsible data handling for achieving the SDGs.[104]

The UN Principles on Personal Data Protection and Privacy of the High-Level Committee of Management (see next section) were developed and unanimously endorsed by the UN PPG.[105]

4.5 Personal Data Protection and Privacy Principles of the HLCM

The ten Personal Data Protection and Privacy Principles, approved by the High-Level Committee on Management (the "Principles") in 2018, are intended to set out a high-level framework for the processing of personal data by, or on behalf of, the United Nations system organisations in carrying out their mandated activities. The Principles were prepared by UN Data Privacy Policy Group (UN PPG), an initiative in which 34 UN entities participated. [106]

The Principles aim to:

- harmonize standards for the protection of personal data across the United Nations System Organizations;
- facilitate the accountable processing of personal data for the purposes of implementing the mandates of the United Nations system organizations, and;
- ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy.[107]

Each of the principles has a corresponding principle in Article 5 of the EU's GDPR.

PERSONAL DATA PROTECTION AND PRIVACY PRINCIPLES OF THE HLCM	
FAIR AND LEGITIMATE PROCESSING	The United Nations System Organizations should process personal data in a fair manner, in accordance with their mandates and governing instruments and on the basis of any of the following: (i) the consent of the data subject; (ii) the best interests of the data subject, consistent with the mandates of the United Nations System Organization concerned; (iii) the mandates and governing instruments of the United Nations System Organization concerned; or (iv) any other legal basis specifically identified by the United Nations System Organization concerned.
PURPOSE SPECIFICATION	Personal data should be processed for specified purposes, which are consistent with the mandates of the United Nations System Organization concerned and consider the balancing of relevant rights, freedoms and interests. Personal data should not be processed in ways that are incompatible with such purposes.
PROPORTIONALITY AND NECESSITY	The processing of personal data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing.

[104] https://www.unglobalpulse.org/policy/un-privacy-policy-group/
[105] https://unsceb.org/privacy-principles
[106] https://www.unicc.org/news/2019/02/11/icc-helps-with-un-principles-on-personal-data-protection-and-privacy/
[107] https://www.unglobalpulse.org/policy/un-privacy-policy-group/

RETENTION	Personal data should only be retained for the time that is necessary for the specified purposes.
ACCURACY	Personal data should be accurate and, where necessary, up to date to fulfill the specified purposes.
CONFIDENTIALITY	Personal data should be processed with due regard to confidentiality.
SECURITY	Appropriate organizational, administrative, physical and technical safeguards and procedures should be implemented to protect the security of personal data, including against or from unauthorized or accidental access, damage, loss or other risks presented by data processing.
TRANSPARENCY	Processing of personal data should be carried out with transparency to the data subjects, as appropriate and whenever possible. This should include, for example, provision of information about the processing of their personal data as well as information on how to request access, verification, rectification, and/or deletion of that personal data, insofar as the specified purpose for which personal data is processed is not frustrated.
TRANSFERS	In carrying out its mandated activities, a United Nations System Organization may transfer personal data to a third party, provided that, under the circumstances, the United Nations System Organization satisfies itself that the third party affords appropriate protection for the personal data
ACCOUNTABILITY	United Nations System Organizations should have adequate policies and mechanisms in place to adhere to these Principles.

The Principles apply to personal data, contained in any form, and processed in any manner. Where appropriate, the Principles may also be used as a benchmark for the processing of non-personal data, in a sensitive context that may put certain individuals or groups of individuals at risk of harms. The United Nations System Organizations ("Organizations") are encouraged to adhere to these Principles and may issue detailed operational policies and guidelines on the processing of personal data in line with the Principles and each Organization's mandate. [108]

According to the Principles, personal data should also be processed in a non-discriminatory, gender sensitive manner and that Organizations should exercise caution when processing any data pertaining to vulnerable or marginalized individuals and groups of individuals, including children. Implementation of the Principles is without prejudice to the privileges and immunities of the relevant Organizations concerned. In adherence with the Principles, the Organizations should conduct risk-benefit assessments or equivalent assessments throughout the personal data processing cycle.

4.6 UN Secretary-General's High-Level Panel on Digital Cooperation

In July 2018, the Secretary-General convened a High-level Panel on Digital Cooperation to advance proposals to strengthen cooperation in the digital space among governments, the private sector, civil society, international organizations, academic institutions, the technical community, and other relevant

[108] https://www.unicc.org/news/2019/02/11/icc-helps-with-un-principles-on-personal-data-protection-and-privacy/

stakeholders. In particular, the Secretary-General requested consideration of how digital cooperation can contribute to the achievement of the SDGs.

The Panel was to raise awareness about the transformative impact of digital technologies across society and the economy and contribute to the broader public debate on how to ensure a safe and inclusive digital future for all, taking into account relevant human rights norms. The final report, entitled "The Age of Digital Interdependence," was submitted in June 2019, and gives recommendations on how the international community could work together to optimize the use of digital technologies and mitigate the risks in five areas: [109]

1. **Building an inclusive digital economy and society** – by 2030, every adult should have affordable access to digital networks, as well as digitally enabled financial and health services. It was recommended that a broad, multi-stakeholder alliance, involving the UN, platform for sharing digital public goods, engaging talent, and pooling data sets, would be created, in a manner that respects privacy, in areas related to attaining the SDGs. Strategies and plans of action should be developed from a set of metrics. [110]
2. **Developing human and institutional capacity** – The Panel recommended the establishment of regional and global digital help desks to help governments, civil society, and the private sector to understand digital issues and develop capacity to steer cooperation related to social and economic impacts of digital technologies.[111]
3. **Protecting human rights and human agency** – The Panel urged the UN Secretary-General to institute an agencies-wide review of how existing international human rights accords and standards apply to new and emerging digital technologies. In the face of growing threats to human rights and safety, including those of children, the Panel called on social media enterprises to work with governments, international and local civil society organizations and human rights experts around the world to fully understand and respond to concerns about existing or potential human rights violations. The Panel called for enhanced digital cooperation to think through the design and application of the standards and principles of transparency and non-bias in autonomous intelligent systems.[112]
4. **Promoting digital trust, security and stability** – The Panel recommended the development of a Global Commitment on Digital Trust and Security to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action.[113]
5. **Fostering global digital cooperation** – The Panel recommended that, as a matter of urgency, the UN Secretary-General facilitate an agile and open consultation process to develop updated mechanisms for global digital cooperation. A multi-stakeholder "systems" approach for

[109] Report of the UN Secretary-General's High-level Panel on Digital Cooperation, p. 7.
[110] Report of the UN Secretary-General's High-level Panel on Digital Cooperation, p. 37.
[111] Report of the UN Secretary-General's High-level Panel on Digital Cooperation, p. 38.
[112] Report of the UN Secretary-General's High-level Panel on Digital Cooperation, p. 38.
[113] Report of the UN Secretary-General's High-level Panel on Digital Cooperation, p. 39.

cooperation and regulation that is adaptive, agile, inclusive and fit for purpose for the digital age was supported.[114]

4.7 Roadmap for Digital Cooperation

Following the issuance of the report, Member States and over 300 entities and organizations were engaged in the preparation of the Roadmap for Digital Cooperation.[115] The Roadmap notes that digital public goods are essential in unlocking the full potential of digital technologies and data to attain the SDGs, and thus high-speed broadband connection to the internet is necessary. Digital public goods platforms are critical to the development of common standards on open data that can guide the private and public sectors on how to provide open access to data sets, ensuring that more data become available as digital public goods, while respecting privacy and confidentiality. [116]

Greater efforts are needed to develop further guidance on how human rights standards apply in the digital age, including through the Human Rights Council, building upon work by the Special Procedures and treaty bodies, OHCHR and diverse stakeholders. Effective personal data protection and the protection of the right to privacy in line with internationally agreed standards are imperative.[117]

The Roadmap states that it is important to protect the right to privacy in the digital space and to take clear actions to do so in the commercial sphere in order to reverse the trend of social media platforms harvesting personal data for commercial purposes. It was stated that a "good" digital identity that preserves people's privacy and control over their information can empower people to gain access to the much-needed services. Initiatives such as the World Bank's ID4D programme and the UN Legal Identity Agenda Task Force can help countries realize the transformative potential of digital legal identification systems.[118]

According to the Roadmap, data protection does not keep up with advances in hacking and espionage, and therefore effective personal data protection and the protection of the right to privacy in line with internationally agreed standards are imperative. The importance of protecting the right to privacy in the digital space, and to take clear actions to do so, is fundamental for private sector actors. More systemically, the current financing model for social media platforms encourages harvesting of personal data for commercial purposes, with content and advertising tailored to individuals' consumption patterns.[119]

It was considered problematic that some digital identity programmes have been designed outside the frameworks of privacy and data protection. As the Roadmap notes, "If digital identity is to become a trusted force for good and used for everyone, it must be built upon a foundation of user agency and choice, informed consent, recognition of multiple forms of identity, space for anonymity and respect

[114] Report of the UN Secretary-General's High-level Panel on Digital Cooperation, p. 39.
[115] Roadmap for Digital Cooperation, p. 4.
[116] Roadmap for Digital Cooperation, p. 5-8.
[117] Roadmap, p. 15.
[118] Roadmap, p. 15.
[119] Roadmap, p. 15.

for privacy, ensuring that there is transparency when an individual's data are used by government and other entities. The adoption of safeguards related to digital identity is critical for governments and the United Nations as they strive to realize its full utility and potential while building trust in its use, including principles of decentralized data storage, identification and authentication, encrypted communications and "privacy by design."[120]

The Roadmap observed that surveillance technologies have, in many situations, allowed for serious breaches of privacy by governments, individuals and the private sector. If the benefits of increased Internet connectivity are to be realized, it is important that all actors, including Member States, the UN system, the private sector and other stakeholders, promote open-source software, open data, open artificial intelligence models, open standards and open content that adhere to privacy and other applicable international and domestic laws, standards and best practices and do no harm.[121]

After close consideration of the Panel's proposals, the following actions were considered to accelerate global digital cooperation, seizing on the opportunities that are presented by technology – while mitigating the risks – so that progress towards achieving the Goals by 2030 can be made collectively.[122]

1. UNITED NATIONS AS CONVENER AND PLATFORM - The UN may serve as a platform for multi-stakeholder policy dialogue on the emerging technologies outlined above. [123]
2. GLOBAL CONNECTIVITY - The UN will make efforts in order to ensure that every person has safe and affordable access to the internet by 2030, including meaningful use of digitally enabled services.
3. DIGITAL PUBLIC GOODS - If the benefits of increased internet connectivity are to be realized, it is important that all actors promote open-source software, open data, open artificial intelligence models, open standards and open content that adhere to privacy and other applicable international and domestic laws, standards and best practices and do no harm.[124]
4. DIGITAL INCLUSION - To ensure that the voices of those who are not fully benefiting from digital opportunities are heard, a multi-stakeholder digital inclusion coalition – an informal network of like-minded Member States, civil society groups, the private sector and other stakeholders on digital inclusion – will be established.
5. DIGITAL CAPACITY-BUILDING - Building on the mapping of existing digital capacity-building initiatives undertaken by UNDP and ITU, which is intended to be expanded, cooperation with UN entities will be carried out to launch a broad multi-stakeholder network to promote holistic, inclusive approaches to digital capacity-building for sustainable development, including a new joint facility for digital capacity development.

[120] Roadmap, p. 15-16.
[121] Roadmap, p. 16.
[122] Roadmap, p. 22.
[123] Roadmap, p. 22.
[124] Roadmap, p. 23.

6. DIGITAL HUMAN RIGHTS - OHCHR will develop system-wide guidance on human rights due diligence and impact assessments in the use of new technologies, including through engagement with civil society, external experts and those most vulnerable and affected.[125]
7. ARTIFICIAL INTELLIGENCE - To address issues raised around inclusion, coordination, and capacity-building for Member States on artificial intelligence, a multi-stakeholder advisory body on global artificial intelligence cooperation will be established to provide guidance.
8. DIGITAL TRUST AND SECURITY - A broad and overarching statement, endorsed by all Member States, in which common elements of understanding on digital trust and security are outlined, could help to shape a shared vision for digital cooperation based on global values. [126]
9. GLOBAL DIGITAL COOPERATION - To make the Internet Governance Forum more responsive and relevant to current digital issues different cooperation bodies should be established.[127]

4.8 Global Data Access Framework

Referenced in the UN Secretary-General's Roadmap for digital cooperation and initially formulated in 2018, the Global Data Access Framework (GDAF) is an example of a multi-stakeholder initiative that aims to create a platform for sharing digital public goods in a manner that respects privacy. Its main objective is to enable data sharing across the public and private sector in a privacy-protective manner by helping to develop and scale AI-driven projects. The GDAF is co-led by UN Global Pulse, The Future Society's AI Initiative, and McKinsey and Company's 'Noble Intelligence' initiative and has over seventy stakeholders, including major technology firms, academic institutions, NGOs, and UN agencies. The GDAF encourages data sharing and contributes to innovative data governance models by advancing robust requirements for privacy protections for all data sharing, and by incorporating novel technical solutions to better protect data.[128]

The GDAF will rely upon a state-of-the-art reference architecture that will be developed through a collaborative multi-stakeholder effort and will enable data to be discovered by AI systems more easily. Through this mechanism, the GDAF intends to enable entrepreneurs, academics, and governments to unlock the potential for big data and AI for good. The GDAF will substantially contribute to innovative data governance models also by incorporating novel technical solutions to better protect data. This dimension of the GDAF will draw upon UN Global Pulse's experience in working with governments and technology companies in developing privacy-protecting data governance frameworks. [129]

4.9 UN Secretary-General's Data Strategy

The Data Strategy of the Secretary-General for Action by Everyone, Everywhere - with Insight, Impact and Integrity (2020 – 2022) aims at building a comprehensive UN data ecosystem to unlock fully digital, technological and innovation potential for better decisions. The Data Strategy aims to foster stronger

[125] Roadmap, p. 24.
[126] Roadmap, p. 25.
[127] Roadmap, p. 25-26.
[128] https://www.unglobalpulse.org/policy/global-data-access-framework/
[129] https://www.unglobalpulse.org/policy/global-data-access-framework/

decision-making and policy advice, greater data access and sharing, improved data governance and collaboration, robust data protection and privacy, enhanced efficiency across UN operations, greater transparency and accountability, and better services for people and the planet.[130] Data protection and privacy is not the main theme of the Data Strategy, but it seems to be an essential component of it.

The Data Strategy of the Secretary-General was approved by the SG's Executive Committee in April 2020, and introduced at the Chief Executive Board in May 2020, to help UN leaders, managers and UN employees all around the world, in a responsible manner, generate more value from the UN's wealth of data for the organization, people and planet.

The Data Strategy was jointly designed by 50 UN entities, and the Strategy represents an essential component of UN reform, aimed at building a comprehensive UN data ecosystem to unlock fully digital, technological and innovation potential for better decisions. The Data Strategy aims to foster stronger decision-making and policy advice, greater data access and sharing, improved data governance and collaboration, robust data protection and privacy, enhanced efficiency across UN operations, greater transparency and accountability, and better services for people and the planet. [131]

The section of the Strategy entitled 'Initial Programmes of the Data Strategy' highlights the three initial priority programmes that the UN family pursues to unlock more of its data potential for people, planet and UN reform. One of them is 'data protection and privacy,' with the two others being 'transparency and accountability,' and 'data for better policy.'

The UN Data Protection and Privacy programme in the Strategy is about implementing a coherent, comprehensive and crosscutting framework that ensures data protection and privacy when data for public good is collected and used. The Data Strategy states that it is important to: [132]

- ensure that data is processed for purposes consistent with mandates, in a manner that respects the rights, including the human rights, of individuals and of groups;
- facilitate further implementation of the UN Personal Data Protection and Privacy Principles;
- harmonize policies and guidelines across the UN system organizations so that best practices prevail;
- ensure transparency in how we process personal data and to foster trust in UN organizations as reliable partners, and;
- support the 2030 Agenda on Sustainable Development Goals and the Decade of Action.

[130] The Data Strategy, p. 3. https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf
[131] The Data Strategy, p. 3.
[132] Data Strategy, p. 60.

4.10 Joint Statement on Data Protection and Privacy in the Covid-19 Response

In late 2020, a number of UN entities came together to issue a joint statement on the importance of protecting sensitive health-related data in the response to Covid-19. The joint statement noted that personal data has an important role in containing the pandemic. The Joint Statement was issued in November 2020 to support privacy protective use of data and technology by the UN in fighting the pandemic. IOM, ITU, OCHA, OHCHR, UNDP, UNEP, UNESCO, UNFPA, UNHCR, UNICEF, UNOPS, UPU, UN Volunteers, UN Women, WFP and WHO supported the adoption of the joint statement, in line with the UN Personal Data Protection and Privacy Principles adopted by the UN System Organizations.[133]

According to the Joint Statement, it has been proved that the collection, use, sharing and further processing of data can help limit the spread of the virus and aid in accelerating the recovery, especially through digital contact tracing. Notwithstanding the seriousness of the COVID-19 pandemic, the organizations consider that any data collection, use and processing by UN system organizations should be rooted in human rights and implemented with due regard to applicable international law, data protection and privacy principles, including the UN Personal Data Protection and Privacy Principles. Any measures taken to address the COVID-19 pandemic should be consistent with the mandates of the respective UN System Organizations and consider the balancing of relevant rights, including the right to health and life and the right to economic and social development. [134]In addressing the challenges of the COVID-19 pandemic, data processing by UN System Organizations should, at a minimum:

Lawfulness, proportionality	Be lawful, limited in scope/time, and necessary and proportionate to specified and legitimate purposes in response to COVID-19.
Confidentiality, security, retention	Ensure appropriate confidentiality, security, time-bound retention and proper destruction/deletion of data.
Due diligence, risk assessment, compliance with intl law/principles	Ensure that any data exchange adheres to applicable international law, data protection and privacy principles, and is evaluated based on proper due diligence and risks assessments.
Lawfulness, fairness, purpose limitation	Be subject to any applicable mechanisms and procedures to ensure that measures taken regarding data use are justified by and in accordance with the afore-mentioned principles and purposes and cease as soon as the need for such measures is no longer present.
Transparency	Be transparent in order to build trust in the deployment of current and future efforts alike.[135]

The Joint Statement was directed to UN system organizations. While aimed to address the challenges of COVID-19, it may serve as a precedent for using a large pool of personal data such as mobile network data and credit card data, and public security surveillance data, to respond to any future crises of a similar scale quickly. The Statement may work as a reminder for governments and others to respect data protection and privacy,[136] especially regarding authorized access to personal data, secure data storage, specified data use, and anonymized individual data dissemination.[137]

5 DATA PROTECTION AND PRIVACY POLICIES AND RELATED ACTIVITIES OF SELECTED UN ENTITIES

In this Chapter, the privacy policies, instruments and capacity building efforts of a number of selected, separate UN entities are reviewed. World Bank privacy guidance is also reviewed here.

5.1 UN Secretariat Departments (Political and Peacebuilding Affairs, Peace Operations, and Economic and Social Affairs)

The UN Secretariat Departments do not have their own data protection and privacy policies specific to each department. The Privacy Notice on the website of some of the Secretariat Departments, such as on the UNDESA website, are the standard UN privacy notice, stating how the Dept collects and processes personal data on its website. The notice states that by accessing the website, certain information about the user, such as Internet protocol (IP) addresses, navigation through the site, the software used and the time spent, along with other similar information, is stored on United Nations servers. The information does not specifically identify the user and the information stored is used internally, only for web site traffic analysis.[138]

In their daily work the Secretariat Departments follow a number of Secretary-General's Bulletins regarding document and processing, including on information sensitivity, classification and handling, and archives and record management, both of which entered into force in February 2007. [139] The Bulletins note that the work of the UN should be open and transparent, except insofar as the nature of information concerned is deemed confidential in accordance with the guidelines set out in the Bulletin. Information deemed sensitive includes:

- Documents created by the UN, received from or sent to third parties, under an expectation of confidentiality;
- Documents whose disclosure is likely to endanger the safety or security of any individual, violate his or her rights, or invade his or her privacy;
- Documents whose disclosure is likely to endanger the security of Member States or prejudice the security or conduct of any operation or activity of the UN, including peacekeeping operations;
- Documents covered by legal privilege or related to internal investigations;

[133] Joint Statement, p. 1. https://www.unglobalpulse.org/wp-content/uploads/2020/11/Joint-Statement-on-Data-Protection-and-Privacy-in-COVID-19-response-Final-12112020-1-3-3.pdf
[134] Joint Statement, p. 1-2.
[135] Joint Statement, p. 2.
[136] Joint Statement, p. 2.
[137] https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-89-strengthening-data-governance-for-effective-use-of-open-data-and-big-data-analytics-for-combating-covid-19/
[138] https://www.un.org/en/sections/about-website/privacy-notice/index.html If the user provides unique identifying information, such as name, address and other information on forms stored on the website, the information will be used only for statistical purposes and is not published for general access. The United Nations assumes no responsibility for the security of this information.
[139] Secretary-General's Bulletin ST/SGB/2007/6 https://undocs.org/ST/SGB/2007/6

- Internal inter-office or intra-office documents, including draft documents, if disclosure would undermine the Organization's free and independent decision-making process;
- Documents containing commercial information, if disclosure would harm either the financial interests of the UN or those of other parties involved;
- Other kinds of information, which, because of their content or the circumstances of their creation or communication, must be deemed confidential.

The three classification levels of UN documents are:

- "confidential" – information or material whose unauthorized disclosure could reasonably be expected to cause damage to the work of the UN;
- "strictly confidential" – information or material whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to or impede the work of the UN;
- "unclassified" – information or material whose unauthorized disclosure could reasonably be expected not to cause damage to the work of the UN.

Classified records that have been transferred to the Archives and Records Management Section maintaining their original classification, shall be declassified as follows:

- "Strictly confidential" documents shall be reviewed on an item-by-item basis by the SG, or by such officials as the SG so authorizes, for possible declassification when 20 years old. Those not declassified at that time shall be further reviewed, every 5 years thereafter, by the SG or by such officials as the SG so authorizes, for possible declassification.
- Records that are classified as "confidential" shall be declassified automatically by the Archives and Records Management Section when 20 years old.

The Bulletins note that hard copies of classified information received electronically must be printed when received and filed and stored, as the original email must. Electronic transmission of classified information shall be performed only through the use of protected means of communication.

With regards to code cables, the March 2020 Standard Operating Procedure on usage, management, and distribution of code cables applies to all entities within the United Nations Secretariat authorized to use code cables as a means of executive-level communication between the UN Headquarters (UNHQ), Offices Away from Headquarters (OAHs), and field locations.[140]

5.1.1 Expert Panel on Technology and Innovation in UN Peacekeeping

In June 2014, the Under-Secretaries-General for Peacekeeping Operations and Field Support asked the Expert Panel on Technology and Innovation in UN Peacekeeping to recommend ways in which technology and innovation could enhance the enterprise's operational effectiveness.[141]

[140] Standard Operating Procedure EOSG/SOP/2020/001, p. 2.
[141] Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping, https://peacekeeping.un.org/sites/default/files/performance-peacekeeping_expert-panel-on-technology-and-innovation_report_2015.pdf p. 3.

The Expert Panel refers to privacy several times in its final report and the Final Report states that UN peacekeeping missions are bound by the provisions of the UN Charter, rules and regulations, international humanitarian and human rights law, as well as the laws of the host country. These include the right to privacy (including domestic and extraterritorial surveillance), the interception of digital communications and collection of personal data. The Expert Panel noted that the High Commissioner for Human Rights recognized a "clear and pressing need to ensure compliance of any surveillance policy or practice with international human rights law, including the right to privacy, through the development of effective safeguards." The Departments should revise the existing SOP and policy on monitoring and surveillance technology to take account of advances in the technology field [142] The Final Report makes recommendations of which the following relate to privacy in three areas:

1. **Safety and security** - The panel recommends updating privacy policy and training in order to appropriately control the collection, use, storage and sharing of information by UN personnel.[143]
2. **Operational imperatives** - Clear policies should be developed, and leadership accountability be established, to help ensure that information is properly and lawfully obtained, stored, used, processed and shared, and that prevailing privacy laws are respected.[144]
3. **Protection of civilians** - Missions must take care to protect sensitive information as well as the privacy of particularly vulnerable individuals in protection scenarios.[145]

5.1.2 United Nations Fundamental Principles of Official Statistics

The Fundamental Principles of Official Statistics ensure that national statistical systems in all UN Member States are able to produce appropriate and reliable data that adhere to certain professional and scientific standards. The Principles were adopted by Resolution 2013/21 of the UN Economic and Social Council (ECOSOC) of 24 July 2013.[146] The ten Principles are as follows:

Principle 1.	Official statistics provide an indispensable element in the information system of a democratic society, serving the Government, the economy and the public with data about the economic, demographic, social and environmental situation. To this end, official statistics that meet the test of practical utility are to be compiled and made available on an impartial basis by official statistical agencies to honour citizens' entitlement to public information.
Principle 2.	To retain trust in official statistics, the statistical agencies need to decide according to strictly professional considerations, including scientific principles and professional ethics, on the methods and procedures for the collection, processing, storage and presentation of statistical data.

[142] Final Report, p. 108-109.
[143] Final Report, p. 112.
[144] Final Report, p. 115.
[145] Final Report, p. 118.
[146] A/RES/68/261, 29 January 2014. https://unstats.un.org/unsd/dnss/gp/FP-Rev2013-E.pdf

Principle 3.	To facilitate correct interpretation of the data, the statistical agencies are to present information according to scientific standards on the sources, methods and procedures of the statistics.
Principle 4.	The statistical agencies are entitled to comment on erroneous interpretation and misuse of statistics.
Principle 5.	Data for statistical purposes may be drawn from all types of sources, be they statistical surveys or administrative records. Statistical agencies are to choose the source with regard to quality, timeliness, costs and the burden on respondents.
Principle 6.	Individual data collected by statistical agencies for statistical compilation, whether they refer to natural or legal persons, are to be strictly confidential and used exclusively for statistical purposes.
Principle 7.	The laws, regulations and measures under which the statistical systems operate are to be made public.
Principle 8.	Coordination among statistical agencies within countries is essential to achieve consistency and efficiency in the statistical system.
Principle 9.	The use by statistical agencies in each country of international concepts, classifications and methods promotes the consistency and efficiency of statistical systems at all official levels.
Principle 10.	Bilateral and multilateral cooperation in statistics contributes to the improvement of systems of official statistics in all countries.

Principle 6 is the only principle that speaks about natural persons and can thus be considered relevant for "personal data." Good practices were drafted to facilitate the application of each principle, and regarding Principle 6:[147]

- measures should be put in place to prevent the direct or indirect disclosure of data on persons, households, businesses and other individual respondents, and;
- a framework describing methods and procedures to provide sets of anonymous micro-data for further analysis by bona fide researchers, maintaining the requirements of confidentiality, is developed.

Regarding Principle 6, UNDESA states that reliable official statistics depend on public co-operation and goodwill to provide accurate and timely information requested in surveys. Such co-operation and goodwill are maintained by protecting the confidentiality of information provided by respondents. The following are considered as key aspects of confidentiality protection:

- maintaining information securely;
- avoiding release of identifiable information in statistical outputs;
- managing access to microdata for statistical research, and;

[147] https://unstats.un.org/unsd/methods/statorg/Principles_stat_activities/principles_stat_activities.asp

- ensuring that individual information is used solely for statistical purposes. [148]

DESA states that all surveys represent a degree of intrusion, which must be justified on the basis of the need for public information on issues of importance. Therefore, privacy, and ensuring that individual information is used solely for statistical purposes, play an important role in statistical activities.[149]

The Global Working Group on Big Data for Official Statistics (of which the UNDESA Statistics Division is a member), is reviewed earlier in this research. The terms of reference of the GWG state that big data sources are recognized as constituting an important part of the data revolution needed to support the monitoring of the SDGs. It is further stated that big data could contribute to improving some aspects of the quality of statistics, such as timeliness and relevance, without compromising their impartiality and methodological soundness. In particular, Fundamental Principles of Official Statistics 1, 5 and 6 are considered to encourage the use of new data source, such as big data.[150]

5.2 UN Economic and Social Commissions (Asia and the Pacific, and Africa)

The UN Economic Commissions also do not collect personal data. When processing human resources-related personal data or other personal data, the Commissions comply with data protection and privacy policies set by the United Nations Office of Information and Communications Technology. [151] Some of the regional initiatives sponsored by the Economic Commissions include the following.

5.2.1 African Union Convention on Cybersecurity and Personal Data Protection

The United Nations Economic Commission for Africa and the African Union Commission spearheaded the development of the African Union Convention on Cybersecurity and Personal Data Protection, adopted by the African Union Heads of States and Governments Summit in 2014. The Convention is based on the continent's needs and adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection. ECA has supported several African countries in the implementation of this Convention. More on this Convention is explained in Chapter 6.

5.2.2 Digital Identity, Digital Trade and Digital Economy initiative

UNECA works with the African Union Commission on a Digital Identity, Digital Trade and Digital Economy initiative to support member countries to fully harness the potential of digital, and to exploit the benefits of digitization for the continent's development. The work is being done in collaboration with partners including the Omidyar Network, the Rockefeller Foundation and the World Bank. [152]

The work builds on ongoing work on the continent, including the strengthening of CRVS systems and the fostering of a vibrant and inclusive digital economy. The Centre of Excellence on Digital Identity, Trade

[148] https://unstats.un.org/unsd/goodprac/bpaboutpr.asp?RecId=6
[149] https://unstats.un.org/unsd/goodprac/bpaboutpr.asp?RecId=6
[150] https://unstats.un.org/bigdata/about/mandate.cshtml
[151] Tanja Sejersen, 28 January 2021.
[152] https://www.uneca.org/dite-africa

and Economy has been established to lead the work and it has many projects under the theme "Development of regulation to safeguard privacy and personal data."[153]

The overriding principles underpinning national digital identity implementations in Africa are the UNECA Framework of Good Digital Identity which stipulates that these systems must be inclusive, privacy-respecting, secure and interoperable with existing and new system.[154] The proposed Principles of Digital ID include the following ten principles of which several principles apply to personal data. [155]

Inclusion	Digital identity systems must be designed and implemented with the rights and interests of all Member States leaving no-one behind. Issue unique identifiers to be recognized everywhere as a person, affirming the principle of non-discrimination and gender equality.
Ownership	Digital identity systems belong to and should remain in the control of all Member States. Each Member State should employ an ownership model that is least vulnerable to external and internal security risks and protecting the rights and security of all identity owners.
Interoperability	Digital identity systems should be interoperable between Member States allowing the unique digital identities authenticated by their own system to recognized by other countries.
Existing systems	Recognition of an individual's identity through the civil registration of major life events. Link the successive issuance of identity credentials and guarantee the legal identity of a person as her/his life progresses.
Privacy	Digital identity systems will be designed to empower individuals and protect online privacy as a fundamental right. The Principle requires consent to capture and process people's data and should be made aware of practices associated with its use and disclosure.
Security and Safeguards	Digital identity systems will incorporate strong security, data protection and privacy laws to secure the identity data of individuals held by the Member States.
Governance	Digital identity systems and the personal data within them should be safeguarded through legal and regulatory framework. Establish the existence of a person under law, and lays the foundation for safeguarding civil, political, economic, social and cultural rights.
Accountability	Periodic and systematic assessment of the completeness and quality of civil registration which will strengthen the ownership and harmonization of digital identity and its applications.
Neutrality	Digital Identity Systems implemented will be built using open standards and will be neutral to any vendor or technology. The advances in technology that allow biometric characteristics of all individuals to be recorded by public and private institutions.

[153] Concept Note, p. 3-4. https://www.uneca.org/sites/default/files/uploaded-documents/DITE-Africa/concept-note.pdf
[154] Concept note, p. 2-3.
[155] https://www.uneca.org/dite-africa/principles-digital-id

Standards	The African Union, the regional economic communities and the United Nations Economic Commission for Africa will work together to create continental and regional standards for digital ID's.

In addition to physical, economic and administrative barriers and legal issues, data privacy breaches, cyber-attacks and cyber-fraud around the world are on rise and impacting productivity, revenue and client trust in the digital economy, and therefore risk undermining the implementation of various development initiatives for digitization in Africa.[156]

5.2.3 Africa Data Leadership Initiative

Launched 6 October 2020, the Africa Data Leadership Initiative (ADLI) is an initiative organized by the UN Economic Commission for Africa, Smart Africa and Future State. It is a peer network designed for and by African policymakers, consumer rights advocates, and private sector stakeholders to ensure that the data economy drives equitable growth and social progress across the African continent. ADLI also contributes to broader initiatives like the African Union-led framework for an African Data Governance Agenda to build a comprehensive data policy for the continent. [157]

Intra-African cooperation was called for to enforce data protection legislation. Data protection is an important subject within the initiative as data is often considered the world's biggest, most expensive and most important commodity and the development of the digital economy amplifies cross-border flows of personal data.[158] African Union Commissioner Dr Amani Abou-Zeid stated, in the event launch, that more highly trained data professionals, data workers who collect, store, analyze, interpret and visualize data, are needed in Africa. All Member States were called upon to ratify the African Union Convention on Cyber Security and Personal Data Protection Convention or to revise existing national strategies to become more inclusive of all data communities.[159]

5.2.4 UNESCAP privacy-related webinars

In an effort to help ASEAN Member States enhance their data privacy regimes, APTICT, the Asian and Pacific Training Centre for ICT, organized a virtual training, Webinar On Data Privacy Laws In ASEAN, in collaboration with the ASEAN Data Protection and Privacy Forum and National Privacy Commission (NPC) of the Republic of the Philippines, from 30 November to 3 December 2020.

The training was to deepen understanding of participants on data privacy regimes and facilitate knowledge-sharing among those ASEAN Member States having and those not having privacy laws. It was also to foster cooperation in developing a harmonized legal environment in ASEAN by identifying key elements of digital privacy laws.[160] The resource materials on data privacy laws in the Asia and the Pacific include information divided in five chapters:

[156] https://www.uneca.org/dite-africa/what-are-challenges-dite-africa
[157] https://futurestate.org/adli/
[158] Press release of the event, p. 1. https://au.int/sites/default/files/pressreleases/39363-pr-pr-_african_union_leading_on_data_economy_in_africa_._for_africa1.pdf
[159] Press Release, p. 2.

i. Privacy in a data driven world;
ii. Comparing regional privacy frameworks: OECD, APEC, ASEAN and GDPR;
iii. Data privacy laws in SELECT ASIA – PACIFIC Economies;
iv. Data privacy laws of ASEAN member states, and;
v. Privacy regulatory landscape in Asia-Pacific.

At the country level, the January 2021 Myanmar Webinar on Data Protection and Privacy was organized with the National Cyber Security Center (NCSC), Information Technology and Cyber Security Department, Ministry of Transport and Communications of Myanmar. The aim of the training was to enhance understanding among policymakers, regulators and civil servants on the importance of data privacy and protection; emphasize the role of data privacy legislation; and share information on international frameworks and good practices, including from ASEAN countries. [161] The February 2021 Samoa Webinar on Information Security and Privacy's aim was to enhance the understanding of civil servants on formulating and implementing information security policies, plans and programmes.[162] A similar webinar will be held for Indonesia in the near future and other national webinars will be decided based on demand from the ASEAN member States, such as Vietnam, Laos, Cambodia and the Pacific Islands. Target audiences for these webinars are policymakers and civil servants of ministries and agencies responsible for data protection and privacy. For ESCAP the biggest challenge with these webinars is to customize the training contents to fit the audience's context as much as possible in order to give practical help. [163]

5.3 International Civil Aviation Organisation

5.3.1 Guidelines on Passenger Name Record Data

ICAO has a key role to play in global policy discussions around data protection and privacy, and the organization has led global technical standard-setting on travel documents (including passports) for many years. Data protection plays an important role in Passenger Name Record data processing. Guidelines on PNR data were approved in 2010, and aim to establish uniform measures for PNR data transfer and the subsequent handling of these data by the States concerned, based on the following principles: [164]

COST MINIMIZATION	Minimization of the cost to industry
ACCURACY	Accuracy of information
COMPLETENESS	Completeness of data
PRIVACY	Protection of personal data
TIMELINESS	Timeliness
DATA/RISK MANAGEMENT	Efficiency and efficacy of data management/risk management

[161] https://www.unescap.org/events/2021/myanmar-webinar-data-protection-and-privacy
[162] https://unescap.org/events/2021/samoa-webinar-information-security-and-privacy
[163] According to Tanja Sejersen, 28/01/2021 by email.
[164] Guidelines, Chapter 2.2.2. https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_en.pdf

According to the Guidelines, States should require PNR data only from aircraft operators who directly operate flights that enter, depart or transit through airports situated in their territories, either as scheduled flights or as the result of an unplanned diversion to an airport situated in their territories. It is considered particularly important to protect PNR data, with the Guidelines proposing States to, as a minimum:[165]

PURPOSE LIMITATION	Limit the use of the data to the purpose for which it collects them.
ACCESS RESTRICTION	Restrict access to such data.
STORAGE LIMITATION	Limit the period of data storage, consistent with the purposes for which data are transferred.
TRANSPARENCY	Ensure that individuals are able to request disclosure of the data that are held concerning them in order to request corrections or notations, if necessary.
REDRESS	Ensure that individuals have an opportunity for redress.
TRANSFERS	Ensure that data transfer protocols and appropriate automated systems are in place to access or receive the data in a manner consistent with the guidelines.

5.3.2 Guidelines on Advance Passenger Information

The Guidelines on Advance Passenger Information were initially developed in 1993 by the World Customs Organization (WCO), the International Air Transport Association (IATA) and ICAO. Further updates have been made in 2003, 2010 and 2013. The goal of the Guidelines is to establish an agreed best practice, to which States and aircraft operators seeking to implement API systems can, to the greatest extent practicable, adhere. [166]

The Guidelines include provisions to address issues such as security, data protection, mutual administrative assistance and 'Interactive API', a more advanced method of passenger processing at airports. It is IATA's view that to achieve the greatest possible efficiency, passenger data exchange processes must evolve to the point where a common and globally agreed data set is collected one time from each person for whom it is required, transmitted once to all having the legal authority to request and view that data, and then used in the most efficient way possible, based on clearly established risk analysis criteria and consistent with acceptable data privacy norms.[167]

Legal aspects of API in the Guidelines state that because of the differences in the provisions and interpretation of privacy and data protection laws from country to country, carriers required to participate

[165] Guidelines, Chapter 2.6.
[166] API Guidelines, p. 3. https://www.icao.int/Security/FAL/Documents/Umbrella_Document.2013Dec03.pdf
[167] API Guidelines, p. 10. https://www.icao.int/Security/FAL/SiteAssets/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards/API-Guidelines-Main-Text_2014.pdf

in API should enquire on a case-by-case basis whether the capture, storage and transmission of the passenger details is in contravention of applicable national law. Where such contravention is determined, the country requiring the API data should, to the best of its abilities, seek to address and resolve those legal concerns.

The Guidelines state that privacy and data protection legislation typically require that personal data undergoing automated processing sets the following five requirements for API data:[168]

Lawfulness, fairness and transparency	Obtained and processed fairly and lawfully.
Purpose limitation	Stored for legitimate purposes and not used in any way incompatible with those purposes.
Data minimization	Adequate, relevant and not excessive in relation to the purposes for which they are stored.
Accuracy	Accurate and, where necessary, kept up to date.
Storage limitation	Preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which that data is stored.

The Guidelines conclude with stating that WCO, IATA and ICAO fully support the effectiveness of API data exchange processes, where adopted in accordance with the Guidelines. Through the efficient use of API data received from carriers and the close co-operation between multiple agencies concerned, API can be the catalyst for increased contact between these agencies and the development of common programmes which can be of benefit from the perspectives of compliance, facilitation, and security. Furthermore, the Guidelines state that agreement on a joint national passenger processing strategy, in which API plays a central role, is of critical importance.[169]

5.3.3 Standards and Principles on the collection, use, processing and protection of passenger name record data

In September 2019, the ICAO Executive Committee stated that the ICAO Guidelines on Passenger Name Record Data cover a wide range of issues related to the transfer of passenger data and that they offer a starting point for the harmonization of the modalities of transmissions of PNR data. However, the Executive Committee considered that the guidelines were insufficient and should be complemented with more far-reaching principles and considerations for the collection, use, processing and protection of PNR data as outlined in the working paper.[170]

The ICAO Executive Committee set out its position on core principles compliance that would ensure respect for the requirements concerning fundamental rights to privacy and data protection when

[168] API Guidelines, p. 25.
[169] API Guidelines, p. 26.
[170] Working Paper A40-WP/530, p. 3-4.
https://www.icao.int/Meetings/a40/Documents/WP/wp_530_en.pdf#search=personal%20data

processing PNR data for the purposes of countering terrorism and serious crime. A growing number of states are requiring airlines to provide PNR data in order to detect and trace the travel routes of criminal and terrorist networks using international air travel. ICAO is taking steps to review and complement the existing standards, recommended practices and additional guidance on the collection, use, processing and protection of PNR data.[171]

The ICAO Executive Committee mentioned that air carriers can face a conflict of laws when confronted with differing legal requirements between states on how personal data must be protected and air carriers can be prevented from transferring PNR data to requesting authorities. The Executive Committee considered that any rules developed to address this issue should ensure that interferences with the right to privacy and protection of personal data are kept to the minimum necessary to achieve its purposes.[172]

Further, the Committee states that the collection and transfer of PNR data affects a large number of individuals against whom there is no prior suspicion, and that such processing should be limited and only allowed under strict conditions in accordance with applicable legal frameworks. While air carriers must always respect legal requirements of the source country, the Committee considered that the following general principles should constitute the basis for the development of ICAO standards in this area:

Lawfulness, fairness and transparency of processing	The need to have a lawful basis for the processing of personal data and to make individuals aware of the risks, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing.
Purpose limitation	The purposes for which PNR data may be used by authorities should be clearly spelt out and should be no wider than what is necessary in view of the aims to be achieved, in particular for law enforcement and border security purposes to fight terrorism and serious crime.
Scope of PNR data	The PNR data elements to be transferred by airlines should be clearly identified and exhaustively listed. This list should be standardized to ensure that such data is kept to the minimum, while preventing the processing of sensitive data, including data revealing a person's race or ethnic origin, politics, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation.
Use of PNR data	The further processing of the data should be limited to the purposes of the original transfer, based on objective criteria and subject to substantive and procedural conditions in line with the requirements applicable to the personal data transfer.
Automated processing of PNR data	Automated processing should be based on objective, non-discriminatory and reliable, pre-established criteria and should not be used as the sole basis for any decisions with adverse legal effects or seriously affecting a person.

[171] Standards and Principles on the collection, use, processing and protection of passenger name record (PNR) data, p. 2. https://www.icao.int/Meetings/a40/Documents/WP/wp_530_en.pdf#search=personal%20data
[172] Standards and Principles on the collection, use, processing and protection of passenger name record (PNR) data, p. 2-3

Data retention	The period of retention of the PNR data should be restricted and not be longer than necessary for the original objective pursued. Deletion of the data should be ensured according to the legal requirements of the source country. At the end of the retention period, the PNR data should be deleted or anonymized.
Disclosure of PNR data to authorized authorities	The further disclosure of PNR data to other government authorities within the same country or to other countries on a case-by-case basis may only take place if the recipient authority exercises functions related to the fight against terrorism or serious transnational crime and ensures the same protections as those afforded by the disclosing authority.
Data security	Appropriate measures must be taken to protect the security, confidentiality and integrity of the PNR data.
Transparency and notice	Subject to necessary and proportionate restrictions, individuals should be notified of the processing of their PNR data and be informed about the rights and means of redress afforded to them.
Access, rectification and deletion	Subject to necessary and proportionate restrictions, individuals should have the right to get access to, and the right to rectification of, their PNR data.
Redress	Individuals should have the right to effective administrative and judicial redress in case they consider their rights to privacy and data protection have been infringed.
Oversight and accountability	The authorities using PNR data should be accountable to and supervised by an independent public authority with effective powers of investigation and enforcement, which should be in a position to execute its tasks free from any influence, in particular from law enforcement authorities.

5.3.4 Amendment 28 to Annex 9 - Facilitation - of the Chicago Convention

The Standards and Recommended Practices (SARPs) for international civil aviation are incorporated into 19 technical annexes to the Convention on International Civil Aviation (the Chicago Convention). The formulation and adoption of SARPs for international civil aviation is the most important legislative function performed by ICAO.

- Standard 9.23 requires the contracting States to develop the capability to collect, use, process and protect PNR and to translate the rules for the practical implementation of this capability in the appropriate internal legal and administrative framework in consistency with the SARPs.
- Standard 9.24 requires contracting States, in full compliance with human rights and fundamental freedoms, to clearly identify the PNR data to be used in their operations and set the purposes for which PNR data may be used by the authorities. Such purposes should be no wider than necessary, including, in particular, border security purposes to fight terrorism and serious crime.
- Standard 9.25 establishes requirements concerning data security and the rights of individuals in relation to the processing of their PNR data, including as regards non-discrimination, the provision of information, administrative and judicial redress, access to data and the possibility to request corrections, deletions or notations.
- Recommended Practice 26 encourages States to notify individuals about the processing of their PNR data and the rights and means of redress afforded to them.
- Standard 9.27 requires contracting States to base the automated processing of PNR data on objective, precise and reliable criteria that effectively indicate the existence of a risk, without leading to unlawful differentiation, and refrain from making decisions that produce significant adverse actions affecting the individuals' legal interest based solely on the automated processing of PNR data.
- Under Standard 9.28, States are required to designate one (or more) competent domestic authorities with the power to conduct independent oversight of the protection of PNR data and determine whether PNR data are being collected, used, processed and protected with full respect for human rights and fundamental freedoms.
- Standard 9.29 precludes States from requiring airlines to collect PNR data that are not required as part of their normal business operating procedures, or to filter such data prior to transmission. It also prohibits the processing of sensitive data – that is, PNR data revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning their health, sexual life or sexual orientation – except in exceptional and immediate circumstances to protect the vital interests of the data subject or of another natural person.
- Standard 9.30 lays down obligations concerning data retention and the de-personalisation and re-personalisation of PNR data, requiring States to only retain the data for a set period as defined in their legal and administrative framework which shall be that period necessary and

proportionate for the purposes for which the PNR data is used, and mask it after an established timeframe.

- Recommended Practice 9.32 suggests a maximum retention period of five years and Recommended Practice 9.33 proposes that PNR data should be de-personalised within six months and no later than two years from the moment it is transferred by airlines.
- Standard 9.33 establishes that PNR data should be, as a rule, transmitted through the less privacy-intrusive push method. It also seeks to minimise burdens on air carriers by limiting the ability of States to impose fines for transmission errors in certain circumstances and by requiring them to limit the number of push times.
- Standard 9.34(a) requires contracting States not to prevent the transfer of PNR data to another contracting State that complies with the Standards. Standard 9.34(b) provides that ICAO contracting States shall retain the ability to maintain higher levels of protection of PNR data, in accordance with their domestic legal framework, and to enter into additional arrangements with other States, in particular with a view to comply with their internal legal requirements.
- Under Standard 9.35, contracting States may be called to demonstrate their compliance with the new Standards upon request from another State.
- Where contracting States determine that they must impede PNR data transfers or fine an air carrier, Standard 9.36 requires them to do so in a transparent manner and with the intent of resolving the situation.
- Recommended Practice 9.37 encourages States to notify others of any significant changes in their PNR programme, including as regards compliance with the SARPs.
- Recommended Practice 9.38 suggests that air carriers are not penalised by States while they attempt to resolve disputes regarding PNR data transfers.[173]

5.4 International Labour Organisation

With regards to visitors to their website, the ILO Privacy Policy includes information on visitor data collected by the ILO, such as automatically collected access information, optional information and information on cookies as well as on the way information is used by ILO. According to the data security commitment ILO does not sell any personally identifiable information volunteered on the ILO site to any third party. To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, ILO has put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information collected online, consistent with the policies of the ILO and all ILO employees who have access to, and are associated with the processing of personal data, are under the obligation to respect the confidentiality of official business matters, including personal data. [174]

[173] https://acsa.cocesna.org/wp-content/uploads/2020/07/071-ENG.pdf

[174] https://www.ilo.org/global/privacy-policy/lang--en/index.htm

5.4.1 Minimum requirements for ensuring privacy and data protection in social protection systems

An ILO Policy Brief seeks to provide concrete recommendations on how the protection of privacy and personal data could be strengthened within specific social protection programmes and social protection systems in general.[175] The Brief notes that social protection programmes require the processing of significant amount of data, which is often of a sensitive nature. Effective data protection within social protection systems requires much more than laws and regulations.

The following specific measures are recommendations to ensure that social protection personnel are familiar with the provisions of the law and know how they should be implemented in the specific case of social protection programmes, which should include:

- development of sector-specific data protection policies and guidelines (specific regulation facilitates the operational duties of staff while freeing them from a need to understand every complexity in general data protection laws or outcome of reform);
- inclusion of data protection provisions in programme operational manuals, and;
- appointment of privacy and data protection committees or officers.

Appointment of privacy and data protection committees or officers is advisable to ensure the implementation of data security controls, monitor Management Information Systems and IT security status and responses to information security incidents. These committees or officers should report directly to the highest authority within the programme or social protection system. ILO recommends that specific privacy and data protection regulations or policies include the following:

PURPOSE SPECIFICATION	The type of information to be processed and the purpose for such information.
STORAGE LIMITATION	How long the information will be retained.
TRANSPARENCY	Who will be able to access the information, and how?
DATA SUBJECT RIGHTS	How individuals access their proprietary information and how they can correct or update it.
COMPLAINTS	Complaints and enquiry systems that include avenues for redress.
COMPLIANCE	Expressly identifying authorities in charge of monitoring compliance.
TRANSPARENCY	How regulations or policies will be promoted among staff.
INCENTIVES & REDRESS	Incentives as well as non-compliance sanctions.

ILO considers that social protection programme beneficiaries should have access to personal data the programme may hold, free from constraint, undue delay or expense. In particular, information should be provided upon request regarding any decisions programme authorities make with reference to applicants or beneficiaries, in particular if such decisions limit or terminate benefit access. [176]

Appropriate institutional, technical and physical measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access should be

implemented by social protection authorities and private entities with access to social protection programme information.[177] In addition, appropriate data-sharing between government agencies, private sector involvement and accountability are discussed in the Policy Brief, and continuous capacity-building and training of programme staff are recommended.[178]

5.4.2 Protection of Workers' Personal Data

The ILO Code of Practice on Protection of Workers' Personal Data was to provide guidance on the protection of workers' personal data and to be used in the development of legislation, regulations, collective agreements, work rules, policies and practical measures at enterprise level. The code of practice was adopted by a Meeting of Experts on Workers' Privacy of the ILO in 1996. The meeting recommended the code of practice to be widely distributed.[179]

The code of practice does not have binding force and does not replace national laws, regulations, international labour standards or other accepted standards. The code applies to the manual and automatic processing of all workers' personal data in public and private sectors. The general principles of the code are: [180]

Lawfulness and fairness	Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker.
Purpose limitation	Personal data should be, in principle, used only for the purposes for which they were originally collected. If personal data are to be processed for purposes other than those for which they were collected, the employer should ensure that they are not used in a manner incompatible with the original purpose and should take the necessary measures to avoid any misinterpretations caused by a change of context.
Security	Personal data collected in connection with technical or organizational measures to ensure the security and proper operation of automated information systems should not be used to control the behaviour of workers.
Automated processing	Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data.
Evaluation	Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance.
Self-assessment	Employers should regularly assess their data processing practices: (a) to reduce as far as possible the kind and amount of personal data collected; and (b) to improve ways of protecting the privacy of workers.
Transparency	Workers and their representatives should be kept informed of any data collection process, the rules that govern that process, and their rights.

[175] Social Protection for All Issue Brief, June 2018. https://www.social-protection.org/gimi/RessourcePDF.action?id=55904
[176] Social Protection for All Issue Brief, p. 1.
[177] Social Protection for All Issue Brief, p. 2.
[178] Social Protection for All Issue Brief, p. 2-3.
[179] Protection of workers' personal data, p. VI https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf
[180] Protection of workers' personal data, p. 1-2.

Training	Persons who process personal data should be regularly trained to ensure an understanding of the data collection process and their role in the application of the principles in this code.
Discrimination	The processing of personal data should not have the effect of unlawfully discriminating in employment or occupation.
Cooperation	Employers, workers and their representatives should cooperate in protecting personal data and in developing policies on workers' privacy consistent with the principles in this code.
Confidentiality	All persons, including employers, workers' representatives, employment agencies and workers, who have access to personal data, should be bound to a rule of confidentiality consistent with the performance of their duties and the principles in this code.
No waiver	Workers may not waive their privacy rights.

In addition to the General Principles the code of practice focuses on the following themes.

On collection of personal data, the code states that although workers are expected to provide truthful information, the code shares the view of many national courts that, especially in connection with hiring procedures, workers are justified in refusing to answer questions that are incompatible with the code. In such cases, the employer bears the responsibility for incomplete or inaccurate responses and, consequently, is not entitled to impose sanctions. Moreover, the employer should not profit from a misunderstanding on the part of the worker as to what is being asked if the worker provides additional or irrelevant information.[181]

Regarding the security of personal data, the code asks for specific organizational and technical measures to ensure that access to personal data can be efficiently restricted and protected against loss and that the data can be safeguarded against any unauthorized use, modification or disclosure stressing that there is no abstract general rule on the measures to be taken. The security measures depend on the particular processing circumstances and employers should adapt their approach regarding security measures to the specific conditions under which personal data are processed.[182]

The restriction of the processing of personal data to specific purposes also limits the duration of storage, and therefore, once the particular aim for which the data were processed has been achieved, they should be destroyed. The restriction of the processing of personal data to specific purposes also limits the duration of storage. Once the particular aim for which the data were processed has been achieved, they should be destroyed meaning that once a candidate has been selected, the data concerning all the other candidates should be destroyed, except where rosters of potential candidates are kept with their approval.

Use of personal data includes references to collection, storage or communication and "any other use." The code states that external communication of data should respect the principle that workers' data

[181] Protection of workers' personal data, p. 17.
[182] Protection of workers' personal data, p. 19.

be processed only for purposes connected with the specific employment relationship. The transmission of data for commercial or marketing is thus prohibited unless the workers concerned have explicitly agreed.[183]

The code speaks about both individual and collective rights. Instead of following the example of most data protection laws, the code on the protection of workers' personal data does not start by affirming the workers' right to know but instead the employer's duty to provide workers with regular information. Individual rights also include the right of rectification or erasure of incorrect data.

According to the code the protection of workers against risks arising from the processing of their personal data and the ability to defend their interests successfully depend to a decisive extent on collective rights. Both the form and the content of these rights must be adapted to national systems of labor relations. Though the workers' interests in respect of data processing may be defended by works councils or trade unions and their representatives and this is what happens in practice.

Whereas employers increasingly entrust specialized agencies with recruitment, protection of the workers' personal data can only be secured if in such cases the personal data principles are also extended to employment agencies. Therefore, the code specifically states that employers should explicitly request that the agencies collect and process the data in accordance with the provisions of the code. [184]

Engaging everyone in strengthening the UN data protection and privacy framework will reduce risks, but also create opportunities to strengthen human rights protection and lead by example. [185] The data protection and privacy landscape will be assessed and strengthened within each organization, with full consideration for human rights and new technologies, through better policy, governance, organization and culture, technology, data management and practice. Data protection and privacy regulations, rules, policies and practices shall be harmonized to ensure optimal compliance and accountability.[186]

5.5 International Organisation for Migration

5.5.1 IOM Data Protection Manual and Data Protection Principles

IOM was one of the first international organizations to develop its own internal guidance concerning data protection, when publishing its Data Protection Principles in 2009. The IOM Data Protection Manual has been updated since that date but the updated version it is not available to the public. According to the Manual, the collection and processing of personal data are necessary components of IOM's commitment to facilitate migration movements, understand migration challenges, and respect the human dignity and well-being of migrants. IOM's data protection strategy seeks to protect the interests of IOM beneficiaries, as well as the Organization itself. The Manual was developed for internal

[183] Protection of workers' personal data, p. 20-21.
[184] Protection of workers' personal data, p. 22-24.
[185] Data Strategy, p. 60.
[186] Data Strategy, p. 61.

use but can be used as a resource tool by other organizations engaging in similar operations.[187] The first part of the Manual includes the IOM Data Protection Principles:[188]

1. LAWFUL AND FAIR COLLECTION	Personal data must be obtained by lawful and fair means with the knowledge or consent of the data subject.
2. SPECIFIED AND LEGITIMATE PURPOSE	The purpose(s) for which personal data are collected and processed should be specified and legitimate and should be known to the data subject at the time of collection. Personal data should only be used for the specified purpose(s), unless the data subject consents to further use, or if such use is compatible with the original specified purpose(s).
3. DATA QUALITY	Personal data sought and obtained should be adequate, relevant and not excessive in relation to the specified purpose(s) of data collection and data processing. Data controllers should take all reasonable steps to ensure that personal data are accurate and up to date.
4. CONSENT	Consent must be obtained at the time of collection or as soon as it is reasonably practical thereafter, and the condition and legal capacity of certain vulnerable groups and individuals should always be considered. If exceptional circumstances hinder the achievement of consent, the data controller should ensure that the data subject has sufficient knowledge to understand and appreciate the specified purpose for which personal data are collected and processed.
5. TRANSFER TO THIRD PARTIES	Personal data should only be transferred to third parties with the explicit consent of the data subject, for a specified purpose, and under the guarantee of adequate safeguards to protect the confidentiality of personal data and to ensure that the rights and interests of the data subject are respected. These three conditions of transfer should be guaranteed in writing.
6. CONFIDENTIALITY	Confidentiality of personal data must be respected and applied at all stages of data collection and data processing and should be guaranteed in writing. All IOM staff and individuals representing third parties, who are authorized to access and process personal data, are bound by confidentiality.
7. ACCESS AND TRANSPARENCY	Data subjects should be given an opportunity to verify their personal data and should be provided with access insofar as it does not frustrate the specified purpose(s) for which personal data are collected and processed. Data controllers should ensure a general policy of openness towards the data subject about developments, practices and policies with respect to personal data.
8. DATA SECURITY	Personal data must be kept secure, both technically and organizationally, and should be protected by reasonable and appropriate measures against unauthorized modification, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer. The safeguard measures outlined in

[187] IOM Data Protection Manual, p. 9. https://publications.iom.int/system/files/pdf/iomdataprotection_web.pdf
[188] Part II of the Manual are the Data Protection Guidelines. Part III includes the Generic Templates and Checklists.

	relevant IOM policies and guidelines shall apply to the collection and processing of personal data.
9. RETENTION OF PERSONAL DATA	Personal data should be kept for as long as is necessary and should be destroyed or rendered anonymous as soon as the specified purpose(s) of data collection and data processing have been fulfilled. It may, however, be retained for an additional specified period, if required, for the benefit of the data subject.
10. APPLICATION OF THE PRINCIPLES	These principles shall apply to both electronic and paper records of personal data, and may be supplemented by additional measures of protection, depending, inter alia, on the sensitivity of the personal data.
11. OWNERSHIP OF PERSONAL DATA	IOM shall take ownership of personal data collected directly from the data subject or collected on behalf of IOM unless otherwise agreed, in writing, with a third party.
12. OVERSIGHT, COMPLIANCE AND INTERNAL REMEDIES	An independent body should be appointed to oversee the implementation of these principles and to investigate any complaints, and designated data protection focal points should assist with monitoring and training. Measures will be taken to remedy unlawful data collection and data processing, as well as breach of the rights and interests of the data subject.
13. EXCEPTIONS	Any intent to derogate from these principles should first be referred to the IOM Office of Legal Affairs for approval, as well as the relevant unit/department at IOM Headquarters.

Regarding Principle 11, the Manual states that the assumption of 'ownership' as an institutional standard will allow IOM to maintain ownership of personal data in the event of ambiguities or silence in contracts with third parties and will also add to the Organization's institutional memory and nurture IOM's unique migration mandate. [189] Principle 11 is unique and controversial; it is difficult to imagine how a piece of personal data could be 'owned' by the controller of personal data.

5.5.2 Other privacy related actions

IOM was part of the Advisory Group and assisted in the drafting of the ICRC Handbook on Data Protection in Humanitarian Action and supported the adoption of the joint statement on Data Protection and Privacy in the COVID-19 Response.[190]

IOM's Community Response App enables individuals to opt-in or opt-out digitally in the field online and offline whenever data, photos or videos are collected. It was designed by and for IOM field staff to help demonstrate the impact of projects by capturing feedback and testimonials of migrants, including their personal journeys, achievements, and challenges. [191]

[189] IOM Data Protection Manual, p. 93.
[190] https://www.iom.int/data-protection
[191] https://www.iom.int/community-response-app

5.6 United Nations Development Programme

5.6.1 UNDP Data Strategy

UNDP's lack of a robust, integrated approach to collecting, storing and using data had hindered its ability to serve Member States, while creating privacy, confidentiality and reputational risks.[192] UNDP's utilization of data is a highly fragmented activity. Lack of centralized governance makes it impossible to coordinate UN-wide responses to local and regional regulations (e.g., GDPR) and to ensure that data is being used ethically and in alignment with Principles outlined in the Strategy. Thus, in February 2021, the UNDP Data Strategy was published for internal use, and represents the first UNDP initiative to provide corporate direction and structure in use and governance of data at all levels of the organization.[193] The Data Strategy seeks to establish a framework to produce norms, standards and policies that guide how data is collected, stored, protected and shared in UNDP. Dedicated support shall be provided through a corporate data architecture, a data network with important resources, as well as guidance on aspects such as privacy and security.[194] The following eight Data Principles are included in the Data Strategy to instruct how to act with personal and non-personal data.[195] Resources related to each Principle follow the Principles.

Safeguard personal data	Embed 'privacy by design' into all data practices. Get informed consent and ensure data are anonymized before publishing.[196]
Uphold the highest ethical standards	Anchor data practices in the UN Charter and international human rights frameworks. Ensure that data processes and partnerships serve the public good.
Manage Data Responsibly	Practice effective data stewardship and governance to ensure sound data quality, security and accountability, in accordance with relevant institutional policies and regulations.[197]
Make data open by default	Make data available as widely as possible and avoid 'data hoarding.'[198]
Plan for reusability and interoperability	Maximise the value of data by ensuring it is usable in multiple domains. Make use of open standards and machine-readable formats in order to improve interoperability.[199]
Empower people to work with data	Provide people with the technology and data literacy skills to be able to effectively work with and understand data. Support governments, local communities and civil society partners to strengthen data and statistical capacities.[200]
Expand frontiers of data	Explore emerging practices and innovative technologies to increase data availability and expand coverage of under-represented groups through data collection and disaggregation.[201]
Be aware of data limitations	Assess gaps, risks and bias in the use of data. Actively question blind spots and potential negative implications of data use.[202]

In terms of implementation of the Data Strategy:

- An 'Executive Champion' will lead the implementation of the Data Strategy in 2021, oversee the growth of UNDP data maturity, and champion effective and ethical use of data;
- A Data Governance Group will be established to provide oversight for the implementation of the Data Strategy, monitor progress of UNDP's data maturity, and resolve data-related issues;
- Guiderails will cover topics such as usage, sharing, privacy, retention, acquisition, compliance, security, management, transparency, standardization, integrations, NDAs and technology.

The UNDP Data Strategy aligns with the UN Data Strategy and responds to the challenge put forth across the UN for "everyone, everywhere" to capitalize on data. Under the guidance of the Data Principles, data will be leveraged more successfully and more responsibly, ensuring that data privacy and protection remain essential. [203] The Data Strategy proposes a Chief Data Officer position to be established in order to foster ecosystem effectiveness, efficiency, impact and compliance. The definition of data privacy policy in alignment with Data Principles is included in the Technology 2021 Action Plan. [204]

5.6.2 UNDP Web Privacy Policy

The UNDP Web Privacy Policy describes UNDP's policy concerning the gathering and sharing of visitors' information through UNDP websites. By visiting these UNDP websites, the user accepts the practices described in the policy. The Policy states that in general, it is not needed to reveal the identity of the user or other personal information. When registering for a newsletter, logging on to certain UNDP sites, requesting information, providing feedback, applying for a job, joining a discussion group or an electronic mailing list, the user will be asked to provide personal information such as name, postal address and e-mail address. This information is collected only with the knowledge and permission of the user, and is kept in various UNDP databases. When donating, credit card details may be requested. The Policy also includes information on use of cookies and security of information. The Policy states that UNDP assumes no responsibility for the security of information. The website of UNDP

[192] UNDP Data Strategy, p. 1-2.
[193] https://www.sparkblue.org/content/data-strategy#
[194] UNDP Data Strategy, p. 4.
[195] https://data.undp.org/data-principles/
[196] Informed Consent https://humansofdata.atlan.com/2018/04/informed-consent/
[197] Responsible Development Data Book https://responsibledata.io/wp-content/uploads/2014/10/responsible-development-data-book.pdf
[198] International Aid Transparency Initiative https://iatistandard.org/en/
[199] Mozilla Science Data Reuse Checklist https://mozillascience.github.io/checklist/
[200] Rethinking donor support for statistical capacity building https://www.oecd-ilibrary.org/development/development-co-operation-report-2017/rethinking-donor-support-for-statistical-capacity-development_dcr-2017-9-en;jsessionid=IFdAaTgZsFKktVLHUtbSAMd-.ip-10-240-5-186
[201] Guide to data innovation for development https://sdgintegration.undp.org/guidedata
[202] An ethics checklist for data scientists https://deon.drivendata.org/
[203] UNDP Data Strategy, p. 32.
[204] UNDP Data Strategy, p. 46.

contains hypertext links to other sites external to the UNDP domain, UNDP assumes no responsibility for those sites either.[205]

5.7 United Nations Joint Staff Pension Fund

According to the UNJSPF Privacy Policy, UNJSPF is committed to protecting the privacy of its participants and beneficiaries and to responsible information handling. The Privacy Policy includes rules on data sharing, data retention, data security, social media and mobile applications. The Privacy Policy is guided by the UN Principles on Personal Data Protection and Privacy. A disclaimer in the Policy states that UNJSPF enjoys the same privileges and immunities as the UN organization and therefore is not bound by legislation in any jurisdiction, nor by the jurisdiction of national courts. UNJSPF is governed solely by its Regulations, Rules and Pension Adjustment System.[206]

UNJSPF has dedicated staff overseeing and maintaining the information management systems and all of the Fund's external and internal processes. The Fund is ISO 27001 compliant and has more than 100 controls regulating all aspects of the Fund's software and hardware, from cryptography to asset management. The Rules and Regulations of the Fund and the information security policy emphasize and define how confidential data must be treated, how information is to be protected and what measures must be taken to guarantee business continuity if there is a disaster.

The website reminds that UNJPSF never sends or asks for personal information such as account numbers, PIN or passwords via e-mail or text messages and gives examples of fraudulent emails of recent years. [207]

5.7.1 Digital Certificate of Entitlement

A new initiative of the UNJSPF is the "Digital Certificate of Entitlement," that ensures effective and timely remote support worldwide to the 80.000 retirees/beneficiaries and 132.000 participants of the United Nations Joint Staff Pension Fund, located in approximately 195 countries. The focus is not on legal frameworks or governance mechanisms. Thanks to the Digital Certificate of Entitlement, retirees and beneficiaries may complete the annual Certificate of Entitlement exercise by providing their annual proof of life in biometric format (facial recognition) through a new Digital Certificate of Entitlement App. The Digital Certificate of Entitlement system is one of the most significant projects of the new Fund's strategy to:

- Simplify client experience;
- Business transformation;
- Develop a global partnership network.

5.8 United Nations High Commissioner for Refugees

UNHCR and its partner organizations process a large amount of information on individual refugees, asylum-seekers, internally displaced persons, and other assisted and protected people in their daily

[205] https://www.undp.org/content/undp/en/home/copyright-and-termsofuse/undp-web-privacy-policy.html
[206] https://www.unjspf.org/privacy/
[207] https://www.unjspf.org/fraud-alert/

work, many of whom are often in a vulnerable position. Their information is highly sensitive and data protection is therefore particularly important to UNHCR.[208]

5.8.1 Policy on the Protection of Personal Data of Persons of Concern to UNHCR

The Policy on the Protection of Personal Data of Persons of concern to UNHCR was adopted in May 2015 as the first data protection instrument of a UN agency.[209] It works as the main data protection instrument for UNHCR staff and lays down the rules and principles relating to the processing of personal data of persons of concern to UNHCR. Its purpose is to ensure that UNHCR processes personal data in a way that is consistent with the 1990 United Nations General Assembly's Guidelines for the Regulation of Computerized Personal Data Files and other international instruments concerning the protection of personal data and individuals' privacy. The Policy is complemented by Operational Guidelines that provide guidance on its implementation, supervision and accountability. [210]

In the Policy, the "Data Controller" is the UNHCR staff member, usually the Representative in a UNHCR country office or operation, who has the authority and accountability for overseeing the management of, and to determine the purposes for, the processing of personal data. When UNHCR works with governments an MoU is usually signed to agree on the processing of personal data and related rights and obligations of the parties. Joint-controller situations can be challenging. Complicated situations may also arise when the host countries have data protection laws with different requirements than the UNHCR data protection tools. In those cases, more stringent requirements are applied.

A "Data Protection Impact Assessment" is a tool and a process to assess the protection impacts on data subjects in processing their data, and for identifying remedial actions to avoid or minimize such impacts. A Data Protection Impact Assessment is usually required to be carried out before the start of any operations where personal data are processed.[211]

The processing of other than personal data, e.g., aggregated or anonymized, does not fall within the scope of the Policy, but is covered, inter alia, by UNHCR's Information Classification, Handling and Disclosure Policy. However, the Policy applies whether processing takes place within one UNHCR office, between different UNHCR offices in the same or more than one country, or whether personal data is transferred to Implementing Partners or third parties and it continues to apply even after persons are no longer of concern to UNHCR. Compliance with this Policy is mandatory for all UNHCR personnel.[212]

UNHCR personnel need to apply the following basic principles when processing personal data:[213]

---

[208] Alexander Beck, Senior Data Protection Officer, on the particular role of data protection for UNHCR. May 23rd, 2018. https://www.unhcr.org/blogs/data-protection-part-parcel-refugee-protection/

[209] https://www.unhcr.org/blogs/data-protection-part-parcel-refugee-protection/

[210] https://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=5b360f4d4

[211] Lea Bardagki, 22 February 2021.

[212] Policy, p. 8.

[213] Policy on the Protection of Personal Data of Persons of Concern to UNHCR, p. 15. 2015. https://www.refworld.org/docid/55643c1d4.html

LEGITIMATE AND FAIR PROCESSING	Processing of personal data may only be carried out on a legitimate basis and in a fair and transparent manner. UNHCR may only process personal data based on one or more legitimate bases.
PURPOSE SPECIFICATION	Personal data needs to be collected for one or more specific and legitimate purpose(s) and should not be processed in a way incompatible with this/those purpose(s).
NECESSITY AND PROPORTIONALITY	The processing of personal data should be necessary and proportionate to the purpose(s) for which it is being processed. Therefore, data that is processed should be adequate and relevant to the identified purpose, and not exceed that purpose.
ACCURACY	Personal data should be recorded as accurately as possible and, where necessary, updated to ensure it fulfils the purpose(s) for which it is processed.
RESPECT FOR THE DATA SUBJECT'S RIGHTS	The data subject's rights to information, access, correction, deletion and objection, are dealt with under Part 3 of the Policy. They include right to information, right of access, correction and deletion and right of objection.
CONFIDENTIALITY	UNHCR personnel needs to maintain the confidentiality of the personal data of persons of concern at all times, even after a data subject is no longer of concern to UNHCR.
SECURITY	In order to ensure the confidentiality and integrity of personal data, appropriate technical and organizational data security measures need to be put in place. Part 4 includes more requirements for data security and confidentiality.
ACCOUNTABILITY AND SUPERVISION	In order to ensure accountability for the processing of personal data in line with this Policy, UNHCR an accountability and supervision structure has been set up. The structure consists of the following key actors: (i) A Data Protection Officer within the Division of International Protection at UNHCR Headquarters, (ii) Data controllers in each country office/operation, and (iii) Data protection focal points in country offices/ operations.

5.8.2 Guidance on Registration and Identity Management

The Guidance on Registration and Identity Management was developed alongside the Policy on Registration and Identity Management and sets out the developments of the past decade in the core activity of the Organization, key to protection and solution outcomes. Its purpose is to support UNHCR staff in the implementation of the afore-mentioned policy, while also providing UNHCR operations, host governments and registration partners with a comprehensive repository of guidance and good practices in registration and identity management. The guidance is published electronically and shall be updated

as necessary over time, ensuring it remains current and aligned with evolving practices, technological advances and UNHCR policy developments in the future.[214]

The Guidance applies to registration and identity management activities for asylum-seekers and refugees covering registration relating to all phases of displacement, from preparedness to pre-registration and emergency registration, to regular registration and biometric enrolment, continuous registration and verification exercises. It also considers a variety of operational settings including emergencies, camp and urban environments and the different scenarios for UNHCR collaboration with governments on registration, from UNHCR-only through to government-only registration procedures. IDP enrolment and registration of other populations of concern are outside the scope of this guidance and the related policy.

Regarding legal framework and political context, the Guidance states that broader considerations are relevant to registration, including inter alia:

- the extent to which data protection and data privacy laws and technical capacity exist, and how they permit or restrict UNHCR's sharing of data/access to data;
- the refugee population data collected by host authorities (or requested of UNHCR) and the purpose it serves;
- initiatives to strengthen civil registration and vital statistics (CRVS) systems;
- laws related to birth registration for foreign nationals;
- how nationality laws function to enable or restrict the passing of nationality to children, and;
- developments in immigration and visa rules.

Regular evaluation of the laws, policies, and institutional capacities in the host country will help UNHCR in an evolving national context, ensure approaches are in line with national developments, highlight the changing constraints and opportunities and facilitate an ongoing assessment as to the interest and/or capacity of host government authorities to assume some or all registration functions over time.

The Guidance is divided into eight modules. Module 3, Planning and Preparing Registration and Identity Management Systems, states that registration should be conducted in an efficient, accountable, fair and transparent manner and recommends considering the following (personal) data related questions:

- Is data collected by the government shared with UNHCR? Is data collected by UNHCR shared with the government? Are there duplications that could be avoided?
- Are there duplicate registration mechanisms in place with other agencies or partners that should be resolved through improved information sharing?
- Are data sharing agreements (DSA) in place with all stakeholders requiring access to registration data?
- Are individuals informed through a clear consent form of all the actors their data may be shared with for assistance and protection purposes?

[214] https://www.unhcr.org/registration-guidance/

- What are the current admissibility criteria for registration, and what procedural safeguards are in place to ensure access to international protection?
- Are screening or pre-screening procedures in place for registration (fighters, host country or third country nationals)? Are these measures necessary and proportionate?
- Are registration Standard Operating Procedures (SOPs) available and regularly updated and shared?
- Are individuals registered within a period of three months?
- What communication and complaint mechanisms are in place?
- What antifraud mechanisms have been established?
- Are adjudication cases being resolved by protection colleagues?

A reference to the Policy on the Protection of Personal Data of Persons of concern to UNHCR is made.[215] In Module 4, Communicating with Communities about Registration, "Confidentiality, data protection and consent" are discussed and following guidance is given:

- Confirm that all personal data collected will be stored confidentially by UNHCR.
- If applicable, inform individuals that basic biodata will be shared with the host government.
- Confirm that personal data will not be accessible to country-of-origin governments without the express consent of individuals concerned.
- Explain that UNHCR may request consent from individuals to share their personal data with partners for the purposes of protection, assistance, and solutions interventions.
- Individuals may refuse consent to share personal data with partners. Explain any impact this may have on access to assistance or other intervention.[216]

Module 7, Working with registration data, gives guidance on data security and data protection: "The personal data of asylum seekers and refugees must be managed in a way that protects confidentiality and is consistent with privacy and data protection principles set out in Part 2 of UNHCR's Data Protection policy."[217]

5.8.3 Data Transformation Strategy 2020-2025

The 2019 UNHCR Data Transformation Strategy 2020-2025 aims to enable UNHCR to lead globally on data protection, security and data ethics, and will ensure that all persons of concern have access to their data and other information to make decisions about their lives.[218] According to the strategy, UNHCR data and information activities will be guided by core principles that are applicable regardless of the type, context, or purpose. Anchored in the overall imperative of "Do no harm", these principles will ensure that the UNHCR activities are consistent with responsible and ethical approaches to data management in humanitarian contexts. The UN's Personal Data Protection and Privacy principles and UNHCR's Data Protection Policy inform all processing of personal data, and UNHCR data and

[215] https://www.unhcr.org/registration-guidance/chapter3/understand-the-context/
[216] https://www.unhcr.org/registration-guidance/chapter4/information-campaigns/
[217] https://www.unhcr.org/registration-guidance/chapter7/registration-data-for-protection-programming/
[218] Data Transformation Strategy, p. 3. https://www.unhcr.org/5dc2e4734.pdf

information activities adhere to high international information and cybersecurity standards, including the concept of privacy, by design and by default.[219]

The Strategy discusses that UNHCR also must ensure that individuals and communities have the data and information needed to enhance their own protection, meet their own needs and identify their own solutions. The fast-changing digital identity landscape calls for new frameworks that facilitate the flow and use of data while also ensuring the right to privacy and data protection.[220]

The objective of the Strategy is that quality and coherent data related to refugees and other persons of concern is systematically, responsibly and efficiently managed by UNHCR and its partners, and shared openly and responsibly both internally and externally. Therefore, data should be processed according to organizational norms and conventions and through well-developed and functional systems and processes. Capacities of staff and partners to oversee data collection and quality, data protection and data analysis should be robust, and roles, responsibilities and authorities of staff engaged in data management in headquarters, regions, and countries clear.

UNHCR demonstrates global leadership and builds capacities and standard protocols on issues of ethical and responsible data approaches, inclusion in digital systems, and identity management, in ways that protect and empower persons of concern. Guidance, including policies and protocols on how personal data is processed, including micro-data, is uniformly applied throughout the organization, and increasingly used by all Member States and implementing partners. Refugees and other persons of concern have increased access to ownership and agency over their personal data. [221]

UNHCR aims to invest in the following four priority areas during the period 2020-2025:

- Data Management and Governance;
- Information Systems;
- Capacities, and;
- Culture.

Investments in information systems should be made leveraging the technology and data trends to ensure data protection and security, data quality and consistency, as well as inter-operability and mutual data transfer with external systems. Some investments that are unique to refugee and stateless populations are needed, while others will be unique to situations of internally displaced persons.[222]

5.8.4 Web Privacy Policy

The UNHCR website includes a privacy policy applying on personal data made available by users of its website. The privacy policy describes what information is made available to UNHCR and third parties when visiting UNHCR web pages on other sites, the use of cookies and how UNHCR uses and stores that

[219] Data Transformation Strategy, p. 6.
[220] Data Transformation Strategy, p. 14.
[221] Data Transformation Strategy, p. 15.
[222] Data Transformation Strategy, p. 16.

information. Any information voluntarily disclosed to UNHCR by users of UNHCR website is held with the utmost care and security and will not be used in other ways than set forth in the privacy policy.[223]

5.9 United Nations Population Fund

The UNFPA Privacy Policy describes UNFPA's policy concerning the gathering and sharing of visitors' information through the UNFPA website and what information is made available to UNFPA and third parties, and how UNFPA uses and stores the information. By visiting the website, visitors consent to UNFPA collection and use of personal and other information as described in the Privacy Policy. The Privacy Policy includes information on anonymous website usage, collection and use of personal data, opting out and changing the user's information, cookies, security and contact information. Also, the Privacy Policy includes information on user generated data which means photos and videos that UNFPA may ask its stakeholders and community to share with the public on the UNFPA website.[224]

5.9.1 Nairobi Summit

UNFPA was involved in the International Steering Committee (ISC) which provided high-level strategic and political guidance for the Nairobi Summit (ICPD25, i.e., International Conference on Population and Development). The Summit was organised in November 2019 in Kenya, to present ambitious commitments with concrete and innovative actions that will accelerate the implementation of the ICPD Programme of Action, leaving no one behind, ensuring rights and choices for all.[225] The Statement coming out of the Summit established 12 commitments to deliver on the promise of the ICPD Programme of Action, the Key Actions for the Further Implementation of the Programme of Action of the ICPD, and the outcomes of its reviews, and the 2030 Agenda for Sustainable Development. Among other things, the Summit committed to draw on demographic diversity to drive economic growth and achieve sustainable development, by:

- Providing quality, timely and disaggregated data, that ensures privacy of citizens and is also inclusive of younger adolescents, investing in digital health innovations, including in big data systems, and improvement of data systems to inform policies aimed at achieving sustainable development;
- Committing to the notion that nothing about young people's health and well-being can be discussed and decided upon without their meaningful involvement and participation ("nothing about us, without us").[226]

5.9.2 Virtual Expert Group Meeting on Access versus Privacy: The Special Case of Population Data

UNFPA, in partnership with the Global Partnership for Sustainable Development Data, Statistical Service Ghana and the Office of the United Nations High Commissioner for Human Rights, co-hosted a virtual event (October 2020) bringing together technical experts, academics, and the general public, to discuss

[223] https://www.unhcr.org/privacy-policy.html
[224] https://www.unfpa.org/unfpa-privacy-policy
[225] https://www.nairobisummiticpd.org/content/about-nairobi-summit
[226] https://www.nairobisummiticpd.org/content/icpd25-commitments

the topic of "Access versus Privacy: The Special Case of Population Data."[227] While the 'data revolution' has been widely embraced, governments are at very different stages in developing and adopting relevant data governance systems, i.e., legislation on data privacy. Some of the topics discussed included:

- Unique Identity systems - risks and benefits;
- Challenges of indigenous self-identification in census;
- Racial and ethnic data in census and implications for tracking inequality;
- Universality and confidentiality: the challenge in a modern census;
- Address and Location Data: Confronting Challenges, Opportunities and managing human rights risks during COVID-19, and;
- Location-based services and the privacy-security dichotomy: case of census mapping during the 2020 census round in Africa."[228]

The Virtual EGM noted that following the global pandemic, the emergence of contact tracing for COVID-19 has highlighted the intersection between societal benefits of population data, and potential privacy concerns. The priority of modern population data for national resilience to any health crises, and the need to simultaneously promote access to ever more granular population data for health and development, while protecting personal data and privacy are therefore reinforced by COVID-19. It has become clear that concerns over unregulated data privacy are hindering public access to critical census, registry, and survey data in countries. Biometrics are increasingly integrated within population data as part of modern legal identity systems and have the potential to validate census and other population data.[229]

Realizing the development potential of such new population data opportunities demands equal attention to the development of robust, nationally tailored data governance. Developing the potential of such new population data opportunities demands equal attention to the development of robust, nationally tailored data governance. It is crucial to protect the safety and security of individuals, particularly for vulnerable populations and minorities - so that data can be accessible to many, but risky to none. Expertise and common guidelines for how to deal with data privacy is therefore a high priority in the context of strengthening population data for development.[230]

5.10 UNICEF

5.10.1 UNICEF Policy on Personal Data Protection

UNICEF uses personal data in a range of activities, whether it is to carry out beneficiaries' needs assessments, to implement child protection programmes, to tailor supporters' engagement or to

[227] https://www.unfpa.org/events/virtual-expert-group-meeting-access-versus-privacy-special-case-population-data

[228] https://www.unfpa.org/sites/default/files/event-pdf/EGM-privacy-vs-access-Agenda.pdf

[229] https://www.unfpa.org/events/virtual-expert-group-meeting-access-versus-privacy-special-case-population-data

[230] https://www.unfpa.org/events/virtual-expert-group-meeting-access-versus-privacy-special-case-population-data

manage human and supply resources. UNICEF must consider opportunities and risks in the use of personal data, including in combination with evolving technologies (e.g., biometrics, artificial intelligence).[231]

The UNICEF Policy on Personal Data Protection[232] is effective since July 2020. It implements the UN principles and governs the processing of personal data by UNICEF. The Policy stipulates a compliance framework for appropriate personal data protection throughout the data life cycle (e.g., collection, storage, analysis, transfer, deletion, or collectively, 'processing'). The Policy applies only to the processing of personal data collected and/or further processed by UNICEF filing systems and provides protection that is appropriate to the risks and sensitivity regarding the personal data processed by particular filing systems. It is intended for internal use.

The Personal Data Protection principles are the following:

Legitimate and fair processing	One or more legitimate bases is required for the processing of personal data.
	Personal data shall be processed in a manner that is transparent to the data subject
Purpose specification	Personal data shall be processed for specified and limited purposes, which are consistent with the mandate of UNICEF and are determined prior to the time of collection.
Necessity and proportionality	The processing of personal data shall be relevant, limited and adequate to what is necessary in relation to the purpose(s) specified for processing. This requires, in particular, ensuring that the personal data collected are not excessive for the purposes for which they are collected, and that the period for which the data are stored in the UNICEF filing system, is no longer than necessary, in conformity with limited retention (paragraph 24 of the Principles).
Accuracy	Reasonable efforts shall be made to process personal data with accuracy and currency. The accuracy of the personal data to be retained shall be reassessed periodically. Frequency of accuracy review will depend on factors such as the relative time sensitivity of the personal data. Determination of reassessment frequency shall be substantiated and documented. Personal data in archives need not be reassessed, corrected or kept current.
Security	Personal data shall be classified in accordance with a contextual assessment of its sensitivity, in accordance with UNICEF information security standards. Appropriate organizational, administrative, physical and technical safeguards and procedures shall be implemented to protect the security of personal data, including against or from accidental or unauthorized destruction, loss, alteration, disclosure, access, or unplanned loss of availability. Such measures may include logging access, changes to or deletion of personal data.

[231] https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf.pdf, p. 1.
[232] https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf.pdf

Limited retention	Personal data shall be retained in the UNICEF filing system: a) Permanently, if and only if the criteria under UNICEF's policies and procedures on archiving are met. b) For the time required to achieve the purposes for which the personal data were collected. Those responsible for stipulating and implementing appropriate retention standards shall substantiate and document: i) how long the personal data is needed for the intended purpose(s), ii) after which period of time the data will become stale or no longer useful for the intended purpose(s), iii) the appropriate retention period for the personal data based on assessment of retention needs, iv) how to safely and appropriately destroy or archive the personal data at the end of the determined retention period. Note: retention periods exceeding 10 years require additional substantiation.
Data subject requests to interact with their personal data	Access, correction, deletion, objection and restriction to processing of personal data, and objection to automated decision-making may be requested, subject to the conditions below, by an individual who provides sufficient evidence of being the relevant data subject or associated child representative.
Accountability	Roles and responsibilities for implementing this Policy appear in Annex 3 which includes information on Deputy Executive Director, data protection/privacy specialists and other roles and responsibilities. A failure to comply with the Policy may amount to misconduct, particularly if the result of gross negligence, recklessness or deliberate conduct. The principle state that UNICEF adopts an appropriate oversight structure to interpret the Policy, in particular, when handling data subjects' requests.

In its interpretation and application to the personal data of a child, the best interest of the child is a primary consideration, and an interpretation and application that does no harm shall be sought.[233] UNICEF personnel shall take particular care in processing the personal data of children and vulnerable categories of data subjects. The processing of particularly sensitive personal data is allowed only where necessary to carry out UNICEF's mandate.[234]

- As a controller, UNICEF may only engage with processors, including UNICEF associates, that provide appropriate commitment and assurance of meeting the requirements of this Policy or equivalent personal data protection standards.
- As a joint controller, UNICEF shall agree in writing with other controllers the responsibilities of each and shall disclose the arrangement to the data subject where appropriate.

[233] The Policy applies solely to the processing of the personal data of living individuals. Note, in some countries the laws apply also regarding deceased individuals.
[234] https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf.pdf, p. 1.

- As a processor, UNICEF will notify data controllers of its data protection requirements and will not knowingly process personal data received in non-compliance with the Policy.
- As for personal data protection compliance and risk, the UNICEF Personal Data Protection Policy is intended as a common denominator and standard to be rolled out in each division and office to ensure that each division/office's work follows the requirements of the Policy.

Annex 1 of the Policy includes definitions and Annex 2 information on requests for access, correction, deletion, objection to a restriction of processing, or objections to automated decision-making. Annex 3 concerns roles and responsibilities for implementing the Policy, as mentioned above.

5.10.2 Procedure for ethical standards in research, evaluation, data collection and analysis

The UNICEF Procedure for ethical standards in research, evaluation, data collection and analysis applies to all UNICEF research, evaluation and data collection and analysis involving human subjects or the analysis of sensitive secondary data as well as to all research, evaluation or data collection processes that are carried out or commissioned by UNICEF sections in partnership or independently. It aims to establish minimum and binding standards for ethical research, evaluation and data collection and analysis processes in UNICEF globally and to ensure effective processes and accountability for ethical oversight of these processes.[235]

The Procedure sets rules for ensuring the protection of, and respect for, human and child rights within all research, evaluation and data collection processes undertaken or commissioned by UNICEF, in order to establish minimum and binding standards for ethical research, evaluation and data collection and analysis processes in UNICEF globally as well as to ensure effective processes and accountability for ethical oversight of these processes. The Procedure does not concern only personal data but has a more general scope regarding research, it applies to all evaluation, data collection and analysis involving human subjects or the analysis of sensitive secondary data.[236]

Procedures relating to 'informed consent' state that when engaging human subjects, informed consent must be sought from all participants. Any project seeking to involve children as either participants, researchers or data collectors must, at minimum, comply with local legislation regarding the age or circumstances which allow for informed consent.[237]

The Procedures relating to Privacy and Confidentiality require measures to ensure participants' privacy during and after the data collection process. Confidential participant information or data that is collected must be securely stored, protected and disposed of. Participants should be given a clear indication of who will have access to their private data and in what form.[238]

[235] The Procedure, p. 1. https://www.unicef.org/media/54796/file

[236] The Procedure, p. 2.

[237] The Procedure, p. 11.

[238] The Procedure, p. 12-13.

5.10.3 Responsible Data for Children (RD4C)

UNICEF and the GovLab at New York University initiated RD4C in December 2018. RD4C aims to build awareness regarding the need for special attention to data issues affecting children and to engage with governments, communities, and development actors to put the best interests of children and a child rights approach at the centre of the data activities. The right data in the right hands at the right time can significantly improve outcomes for children but one must ensure that the collection, analysis and use of data on children does not undermine these benefits. [239]

A Synthesis Report synthesizes key findings of the RD4C initiative. The child rights organizations around the world use biometrics, digital identity systems, remote-sensing technologies, mobile and social media messaging apps, and administrative data systems, among other technologies to provide aid that generate data that includes potentially sensitive data, such as personally identifiable information and demographically identifiable information —data points that enable the identification, classification, and tracking of individuals, groups, or multiple groups of individuals by demographically defining factors.[240]

The Synthesis Report states that children typically do not have full agency to make decisions about their participation in programs or services which may generate and record personal data. Children may also lack the understanding to assess a decision's purported risks and benefits. Privacy terms and conditions are often barely understood by educated adults, let alone children. As a result, there is a higher duty of care for children's data. Disaggregating data according to socio-demographic characteristics can improve service delivery and assist with policy development but it creates risks for group privacy. The Synthesis Report states that more than just a concern for digital activities, the ongoing accumulation of data about children throughout their lifetime can create a variety of unforeseen risks and challenges. [241] The RD4C principles reflect elements of the UN Principles on Personal Data Protection and Privacy each RD4C principle having a corresponding principle in the UN Personal Data and Privacy Principles:[242]

PARTICIPATORY vs. Fair and Legitimate Processing	Engaging and informing individuals and groups affected by the use of data for and about children. Responsible data is participatory. It seeks and builds with inputs from those who use and are affected by data, namely children, their caregivers, and the communities in which they live. Accordingly, actors should inform and engage with individuals and groups. In seeking input, actors should pay attention to marginalized and vulnerable population segments as well as to the inputs of partners, donors and other key stakeholders.
PROFESSIONALLY ACCOUNTABLE vs. Transparency and Accountability	Operationalizing responsible data practices and principles by establishing institutional processes, roles, and responsibilities. Data responsibility rests upon broader foundations of professional accountability. To ensure that the practices and principles described above are put in action, and the unique considerations of responsible data for children are operationalized within institutional processes, organizations and partners should collect, process, and use data within a more general culture of data responsibility. Such a culture has many elements, but one of the most important is to establish and clearly define the role of organization-wide data stewards. Data stewards are an emerging role; they are individuals or groups whose duties

[239] Synthesis report, November 2019. https://rd4c.org/files/rd4c-report-final.pdf

	cut across departments and functions, and whose broad remit is to oversee responsibility and accountability in the way data is handled.
PEOPLE-CENTRIC vs. Fair and Legitimate Processing	Ensuring the needs and expectations of children, their caregivers, and their communities are prioritized by actors handling data for and about them. Much of the data used for drawing insights to improve children's lives involves or is generated by people. The insights from it have the potential to impact the lives of children in many ways, both positive and negative. Actors must thus ensure the needs, interests and expectations of people—including children and their caregivers in particular—are prioritized by those handling data about them. Actors should take a people-centric approach to the consideration of opportunities and risks of data initiatives—prioritizing the consideration of data practices' effects on people over potential efficiency gains or other process-oriented objectives. This entails some combination of the following criteria: children and/or their caregivers have consented to the data use, children and/or their caregivers have a clear understanding of how this work will be conducted, the work is demonstrably serving children's interests, and/or the work is required by law or institutional mandate. In addition, actors need to be context sensitive, paying attention to and acting according to the legal, cultural and community contexts in which any given project exists.
PREVENTION OF HARMS ACROSS THE DATA LIFE CYCLE vs. Transfers, Security, Accuracy and Confidentiality	Establishing end-to-end data responsibility by assessing risks during the collecting, storing, preparing, sharing, analyzing, and using stages of the data life cycle. Data is not static but exists on a cycle. As part of a commitment to data responsibility, actors should assess and seek to prevent risks across the full data life cycle, including the collecting, storing and preparing, sharing, analyzing and using stages. This concept is called end-to-end data responsibility. It is essential for preventing harm to children and ensuring trust.
PROPORTIONAL vs. Proportionality and Necessity, Retention	Aligning the breadth of data collection and duration of data retention with the intended purpose. In the data space, less can sometimes be more. When developing and implementing data initiatives, actors should always consider necessity and whether there is proportionality in the breadth of data collection and duration of data retention in order to achieve the intended purpose. The collection and retention of data should be relevant, limited and adequate to what is necessary for achieving intended purposes. The importance of targeting and minimizing collection is true of all data, but especially true of data related to children, given potential and actual vulnerabilities.
PROTECTIVE OF CHILDREN'S RIGHTS	Recognizing the distinct rights and requirements for helping children develop to their full potential. When it comes to children, responsible data practices begin by recognizing their distinct needs and requirements. Children's rights must be realized in order for them to develop to their full potential. Realizing these rights can be complex

[240] Synthesis report, p. 5. https://rd4c.org/files/rd4c-report-final.pdf
[241] Synthesis Report, p. 3 and 12.
[242] Synthesis Report, p. 50.

vs. Confidentiality and Security, Transparency	given children's inherent vulnerabilities, the likelihood that others are making impactful decisions on their behalf, and the future prospects they can achieve if supported effectively by those working in their interest.
PURPOSE-DRIVEN vs. Purpose Specification, Fair and Legitimate Processing	Identifying and specifying why the data is needed and how the intended or potential benefits relate to improving children's lives. A responsible data practice starts by being purpose driven. When seeking to handle data actors should identify and specify why the data is needed and how the intended or potential benefits relate to improving children's lives. If there is no clearly articulated benefit for children, actors should not collect data, store, share or analyze it.

The RD4C work is specifically focused on capacity building as a public good – with a strong field emphasis. Several national governments have shown interest to this initiative even though national governments are not specifically targeted.

5.10.4 Guidance on the use of biometrics in children-focused services

Biometric technology presents a broad range of potential benefits but poses a specific risk to children – above and beyond the data protection and privacy concerns that apply to all biometric applications. This technology has been largely designed to work with adults and may not perform as well when used with children. Errors in biometric recognition can result in potential exclusion from important services and create additional barriers for marginalized and vulnerable groups.[243]

"Faces, Fingerprints and Feet" gives guidance on assessing the value of including biometric technologies in UNICEF-supported programmes. It outlines the 10 key questions and criteria that UNICEF programs are encouraged to ask when evaluating whether to invest or support the use of biometric technologies as part of our own programming. The questions help weighing up the benefits and risks and ensure that appropriate management strategies are in place so that biometrics can be used safely.

UNICEF's engagement with biometric technology is very new and overall, there is very little publicly available evidence on the recognition accuracy of biometric systems, or on the practical and ethical considerations when using such systems with children. There is also a lack of global standards on the best use of such technologies, especially when applied to vulnerable groups such as children. However, work is happening through several UN collaborations, and there is a range of existing standards that can inform the use of new technologies and data principles more generally, even in the absence of specific guidance on biometrics. [244]

Guidance on "Biometrics and Children" is a literature review of current technologies which is prepared by UNICEF and the World Bank (but not yet published). The document examines the publicly available literature on the performance of biometric technologies for children (0-18 years). The level of evidence available and performance metrics is provided for key biometric traits commonly proposed for use with children including facial recognition, fingerprints, iris scans, foot and palm prints. Key findings from the

[243] https://data.unicef.org/resources/biometrics/

[244] https://data.unicef.org/resources/biometrics/

study highlight that while biometric technologies have some application in children above 5 years of age, solutions at younger ages are largely experimental and require more research. The work highlights the critical lack of verifiable performance data on most of the technologies currently in use with children (particularly for longitudinal use over extended periods), and the need for more transparency and critical assessment of the impact of population-scale applications. [245]

5.10.5 Privacy, protection of personal information and reputation

The 2017 Discussion paper "Privacy, protection of personal information and reputation" is included in series of discussion papers on Children's Rights and Business in Digital World. It handles privacy in the world of internet and is divided into following four parts: [246]

- Children's right to privacy under international law;
- Threats to children's rights online;
- The responsibilities of and opportunities for the ICT sector, and;
- The roles of states.

If the relationship between privacy and the Internet is complex for adults, it is doubly so for children. Children's privacy online is placed at serious risk by those who seek to exploit and abuse them, using the Internet as a means to contact and groom children for abuse or share child sexual abuse material. The Discussion Paper states that with respect to informational privacy children should be offered even more robust protection than in general.[247]

According to the part four of the Discussion Paper governments have an obligation to ensure that businesses respect children's rights and should take appropriate steps to prevent and redress abuses of children's rights to privacy, the protection of personal information and reputation online. It proposes different legislative, enforcement and policy measures to improve privacy and protection of personal information and reputation of children. The legislative measures the Discussion Paper proposes include legislation regarding:[248]

- Harassment and misuse of personal information;
- Data Protection;
- Surveillance;
- Open data and freedom of information.

To ensure that laws are enforced as effectively online as they are offline, the Discussion Paper proposes governments to provide regular training for judges, lawyers and police on new developments in technology that incorporate an understanding of children's rights in a digital world. The policy measures include developing guidelines for business entities, privacy impact assessments and reviewing child

[245] https://data.unicef.org/resources/biometrics/
[246] The Discussion Paper Privacy, Protection of Personal Information and Reputation
https://sites.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf
[247] Discussion paper, p. 4 and 9.
[248] Discussion Paper, p. 25-26.

protection measures. The Discussion Paper concludes that businesses and governments alike should adopt measures to better protect and empower children as full rights-holders in a digital world.[249]

5.10.6 Other privacy related work

A range of privacy related work is underway across UNICEF - including the creation of legal templates for safe and responsible data sharing, technical work to address specific issues as part of UNICEF's data-sharing agreements with other agencies and work related to bots in data collection which is a specific high-risk area.[250] UNICEF also works with the UN Data Strategy working groups on data protection and data sharing and has started on several initiatives, such as a personal data inventory workstream to map data flows and data handling throughout UNICEF. UNICEF also works on appropriate privacy notices for its initiatives. The UNICEF Personal Data Breach procedure has been approved which is a key requirement under the Policy. The data breach procedure applies to all UNICEF staff and sets standards for personal data breach reporting, investigation, review, mitigations and notifications. In addition, a DPIA process, data protection training and extension of the inventory workstream to the regions and country offices are under work.[251]

5.11 UN Women

A short (standard UN) privacy notice on the website of UN Women states that certain information of the User accessing the sites will be stored on United Nations and web analytics servers. Such information includes Internet protocol (IP) addresses, navigation through the Site, the software used, and the time spent, along with other similar information. Further it is stated that the information will be used internally only for website traffic analysis. Should the User provide unique identifying information, such as name, address and other information on forms stored on the Site, the information will be used only for statistical purposes and will not be published for general access. The United Nations assumes no responsibility for the security of such information.[252]

5.11.1 Information security

The information security notice on the website of the UN Women states that UN Women is committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information assets held through the organization, not only to support and enable its mandate, strategic objectives, and daily operation, but also to protect its stakeholders. [253]

5.11.2 Other privacy related engagements

UN Women is currently working on a policy and procedure for personal data protection and privacy. The policy will apply internally, i.e., state how UN Women processes personal data. The policy and procedure are based on the UN Personal Data Protection and Privacy Principles, which UN Women has already endorsed and is applicable until the UN Women own policy is finished. Currently UN Women is

[249] Discussion Paper, p. 26-27.
[250] Karen Carter, 21 January 2021.
[251] Sigrun Kaland, 21 January 2021.
[252] https://www.unwomen.org/en/about-the-website/privacy-notice
[253] https://www.unwomen.org/en/about-the-website/information-security

not engaged in big projects related to provision of technical assistance or strengthening the capacity of the protection of personal data of national governments.[254]

5.12 World Food Programme

5.12.1 WFP Guide to Personal Data Protection and Privacy

In emergencies, WFP is often first on the scene, providing food assistance to the victims of war, civil conflict, drought, floods, earthquakes, hurricanes, crop failures and natural disasters. In carrying out its mandate, WFP processes a large amount of information, including personal data of its beneficiaries and prospective beneficiaries. Protecting this information is a fundamental part of WFP's duty of care to those it serves. Breaches in confidentiality could have dire consequences for individual beneficiaries or beneficiary communities, ranging from abuse and ostracization to death.[255]

The WFP Guide to Personal Data Protection and Privacy is a comprehensive guide on data protection being intended for the protection of beneficiaries' personal data in WFP's programming. The Guide is developed for all WFP personnel involved in the processing of data concerning actual or potential beneficiaries. It covers data protection principles and the application of those principles.[256]

The WFP Guide sets the following five principles for data processing:

Lawful and Fair Collection and Processing	WFP shall collect and process personal data by lawful and fair means with the informed consent of the beneficiary.
Specified and Legitimate Purpose	WFP shall collect personal data only for specific, explicit and legitimate purposes and shall further process it in a way that is compatible with those purposes. If a secondary purpose arises that is not compatible with the originally stated purpose, then beneficiary consent must be obtained for this secondary purpose.
Data Quality	WFP shall ensure that personal data sought and obtained is adequate, relevant and not excessive in relation to the specified purpose(s) of data collection and data processing. WFP shall take all reasonable steps to ensure that personal data is accurate and up to date.
Participation and Accountability	WFP shall ensure that beneficiaries are consulted about the processing of their personal data before and during all stages of such processing. Beneficiaries shall be enabled to access, verify, correct, update and erase their personal data. WFP shall ensure confidentiality of beneficiary personal data.

[254] Lene Jespersen, 3 February 2021.
[255] The Guide, p. 1.
[256] WFP Guide, p. 7. https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

Data Security	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.

The Guide provides instructions on specific application of the principles – in particular on Informed Consent, Third-party Data Sharing, Media, on the role as Data Controller or Data Processor, Retention and Disposal of data.[257] It also gives information on how to conduct a Privacy Impact Assessment.[258]

5.12.2 Other privacy guidance

The Guide to Personal Data Protection and Privacy is the key reference for data protection at WFP. For the moment WFP is not providing technical assistance or have actual project to strengthen the capacity of the protection of personal data of national government counterparts. Such capacity building could be part of WFP digital advisory and assistance offerings to Governments. The subject is being discussed internally but WFP staff's skills need to be reinforced first. Limited institutional capacities and financial resources are the greatest challenges of the WFP. [259]

5.13 World Health Organisation

5.13.1 Policy Statement on Data Sharing in the Context of Public Health Emergencies

The Policy Statement on Data Sharing by WHO in the Context of Public Health Emergencies ("the Policy Statement") was published in April 2016. The primary purpose of data sharing by WHO during a public health emergency is to permit analyses that allow the fullest possible understanding of the emergency, and to ensure that decisions are based on the best available evidence.[260] The Policy Statement sets out WHO's position with regard to providing access to data in the following three categories:

- surveillance, epidemiology, and emergency response including health facilities;
- genetic sequencing, and;
- observational studies and clinical trials.

The Policy Statement does not cover other kinds of data that could be useful, but which are not typically provided to WHO, such as telephone Call Detail Records (CDR). Furthermore, the Policy Statement refers to the sharing of data only, not biological samples (which require different considerations).

For surveillance, epidemiology and emergency response data, the Policy Statement applies to data and information received by WHO under Part II of the 2005 International Health Regulations (IHR). The data related to surveillance and monitoring (informing epidemiology), from the emergency response (e.g., contact tracing, vaccination, treatment), and data concerning health facilities (e.g., the numbers and

[257] WFP Guide, p. 45-83.
[258] WFP Guide, p. 85-93.
[259] Silvia Moreira, 2 February 2021.
[260] Policy Statement on Data Sharing by the WHO in the Context of Public Health Emergencies, p. 2. https://www.who.int/ihr/procedures/SPG_data_sharing.pdf

locations of in-patient and out-patient centres, and the staff and medical facilities available at these centres) can be made publicly available when both of the following apply: [261]

(1) the requirements for making the information available to the IHR (2005) States Parties are fulfilled, i.e., when:

- Public Health Emergency of International Concern is declared,
- Evidence indicates that there is, or will be, international spread of infections or other harmful agents or,
- There is immediate need for international control measures, and

(2) other information about the event has already become publicly available and there is a need for the dissemination of authoritative information.

WHO states that such personal data is anonymized to protect privacy and to ensure confidentiality. Anonymization removes all personal identifiers and locators and ensures compliance with the personal data protection requirements as laid out in Article 45 of the IHR (2005) are complied. Efforts will be made to curate data so as to increase their utility, and further analysis and reporting of new data generated will be encouraged. In exceptional cases, where there is a compelling reason to opt out of sharing for subsets of data, this will be possible. [262]

The sharing of genetic sequence data / information is as important as the sharing of other event-related information above. Sharing this data allows the better tracking of epidemics, and aids the development of diagnostic tests, therapeutics and vaccines. [263]

Observational and clinical studies relate to data generated under research protocols and its early sharing of these data in emergencies is not important in the same way that it is for epidemiological and genetic sequence data. Nevertheless, during a public health emergency, WHO's position will be that the public disclosure of results will be the norm, in the expedited timeline as dictated by the research protocol. Outside public health emergencies the norm is for public disclosure of results within 12 months of completion of a trial. [264]

WHO has a formal and comprehensive policy for securely managing all data bases and information sources hosted by the Organization. The policy includes information security, technical and physical data security, data access and retention procedures, and confidentiality arrangements. As international civil servants, all WHO staff are required to adhere to the policy and its procedures (detailed under Staff Regulations), including with full respect to Article 45 of the IHR (2005).[265]

WHO's functions in times of public health emergencies are further elaborated in the IHR (2005) adopted by all of WHO's Member States. Article 45 of the IHR (2005) provides for treatment of personal data as follows:

[261] Policy Statement, p.2.
[262] Policy statement, p. 2-3.
[263] Policy statement, p. 3.
[264] Policy statement, p. 3-4.
[265] Policy statement, p. 4.

1. Health information collected or received by a State Party pursuant to these Regulations from another State Party or from WHO which refers to an identified or identifiable person shall be kept confidential and processed anonymously as required by national law.

2. Notwithstanding paragraph 1, States Parties may disclose and process personal data where essential for the purposes of assessing and managing a public health risk, but State Parties, in accordance with national law, and WHO must ensure that the personal data are:

   - processed fairly and lawfully, and not further processed in a way incompatible with that purpose;

   - adequate, relevant and not excessive in relation to that purpose;

   - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate, or incomplete are erased or rectified, and;

   - not kept longer than necessary.

3. Upon request, WHO shall as far as practicably provide an individual with his or her personal data referred to in this Article in an intelligible form, without undue delay or expense and, when necessary, allow for correction.

5.13.2 Policy on use and sharing of data collected in Member States by the WHO outside the context of public health emergencies

The constitutional functions of the WHO are, among others, to "establish and maintain such administrative and technical services as may be required, including epidemiological and statistical services, to promote research in the field of health, and to provide information in the field of health". More specifically with regard to statistical and epidemiological data, under Article 63 of the WHO Constitution, each Member State "shall communicate promptly to the Organization important (…) statistics pertaining to health which have been published in the State concerned." Article 64 provides that each Member State "shall provide statistical and epidemiological reports in a manner to be determined by the Health Assembly." Article 65 states that each Member State "shall transmit upon the request of the Executive Board such additional information pertaining to health as may be practicable."

The WHO Policy on use and sharing of data collected in Member States outside the context of public health emergencies was approved on 22 August 2017.[266]

The Policy applies to data provided to WHO by Member States, other than data which are published by Member States without any restrictions on their use. The Policy discusses data sharing benefits and measures to mitigate potential risks. It covers the use and sharing of data which does not include biological samples and covers the use and sharing of data collected by WHO in, and/or provided to WHO by, Member States, outside the context of public health emergencies. The Policy expressly

[266] The Policy on use and sharing of data collected in Member States by the WHO outside the context of public health emergencies, p. 2. https://www.who.int/docs/default-source/publishing-policies/who-data-sharing-policy-collected-by-member-states-outside-of-public-health-emergencies61d03608e6134ba786ad94403e947013.pdf?sfvrsn=bb52b31d_31

excludes data shared in the context of public health emergencies, including officially declared PHEICs under the International Health Regulations (2005) and data and reports from clinical trials.[267]

Usually, the compilation, analysis and sharing of aggregated data (e.g., groups of patients or health facilities) does not raise ethical concerns or present risks with regard to confidentiality. However, for data aggregates comprising small numbers of individuals, WHO will ensure that anonymity is preserved:

- by adopting standard security measures;
- by detailing how the data will be received by WHO, and;
- by stating how the data will be shared (including the use of minimum numbers of patients).

In contrast, data on individuals (e.g., patients, survey respondents) provided by Member States may contain personally identifying information. Therefore, that data and other information deemed sensitive (e.g., detailing specific locations or facilities), will be made available by WHO to third parties only after the removal of identifying details following a formally verified anonymization procedure. [268]

In addition, ethical obligations include but are not limited to:

- anonymization, and other tools to protect privacy and confidentiality;
- compliance with informed consent agreements in cases where informed consent is needed and respecting assurances to patients, research participants and other relevant parties about ways in which data (anonymized or otherwise) would be used, shared, stored or protected, and legitimate expectations such individuals may have about these standards;
- avoidance of stigmatization or exclusion of people or communities as a result of data collection;
- adoption of appropriate security measures to foster public trust.

WHO has a formal and comprehensive policy for securely managing all databases and information sources hosted by the Organization. The policy includes information security, technical and physical data security, data access and retention procedures, and confidentiality arrangements. All WHO staff are required to adhere to the policy and its procedures (detailed under the WHO Staff Regulations). [269]

Annex 3 to the Policy contains a standard text for inclusion in data collection forms, which (if used) ensures that WHO has rights:

- to publish the data, stripped of any personal identifiers and make the data available to any interested party on request (to the extent they have not, or not yet, been published by WHO) on terms that allow non-commercial, not-for-profit use for public health purposes (provided always that publication of the data shall remain under the control of WHO);
- to use, compile, aggregate, evaluate and analyse the data and disseminate the results thereof in conjunction with WHO's work, in accordance with the Organization's policies and practices.

[267] The Policy, p. 5-6.
[268] The Policy, p. 6.
[269] The Policy, p. 7.

5.13.3 WHO Data Principles

Article 2 of WHO's Constitution sets out responsibilities and duties that require robust data governance processes. Functions that depend on data-sharing include:

- to act as the directing and coordinating authority on international health work;
- to establish and maintain such administrative and technical services as may be required, including epidemiological and statistical services;
- to promote and conduct research in the field of health;
- to provide information, counsel and assistance in the field of health, and;
- to assist in developing an informed public opinion among all peoples on matters of health.[270]

The collection, analysis, publication and dissemination of health-related data is a core part of WHO's mandate. The WHO Data Principles were published in August 2020 and provide a foundation for continually reaffirming trust in WHO's information and evidence on public health. The following five Data Principles are designed to provide a framework for data governance for WHO and intended primarily for use by WHO staff in order to help define the values and standards that govern how data that flows into, across and out of WHO is collected, processed, shared and used:[271]

1. WHO shall treat data as a public good	WHO shall make every effort to release data publicly and to share when safe and ethical to do so. Unless there is a legitimate justification to the contrary, WHO shall make data open and accessible to the public in line with data being a public good. This principle also applies to data such as vital registration, survey data and the results of estimation and research, and situations in which data have been shared with WHO by non-Member State entities (including private-sector data producers) that collaborate with WHO on common projects.
	Clear guidance shall be provided and transparency ensured. In situations where legitimate reasons prevent the sharing of data, WHO will provide clear guidance on other possible ways in which the data may be accessed, such as for research purposes. For personal data, the consent of the data subject should be the preferred basis for processing the data. WHO shall be transparent about how data are collected, used and shared. The following guidance relates to this topic: • WHO Guidelines on Ethical Issues in Public Health Surveillance;[272] • Information Disclosure Policy;[273] • Policy on use and sharing of data collected in Member States by the WHO outside the context of public health emergencies, and; • WHO Policy on Open Access.[274]
2. WHO shall uphold Member States' trust in data	WHO shall uphold the trust placed in it by Member States when WHO processes data that Member States have shared with it and placed under WHO's control.
	WHO will: - **Provide impartial and inclusive consultation** - **Secure storage and processing** - **Apply human rights and the right to privacy**

	WHO upholds the highest standards of data protection and respect for human rights, including the right to privacy, with regard to any personal data and data aggregates of groups of individuals included in WHO-controlled data sets. This is especially important for data sets requiring careful handling and particular attention, such as sensitive medical data, and data on vulnerable and marginalized individuals and groups, including children. Member States and non-State actors who share data with WHO are required to confirm that the data have been collected in accordance with applicable national laws, including data protection laws aimed at protecting the confidentiality of identifiable persons.
3. WHO shall support Member States' data and health information systems capacity	WHO shall support Member States' capacity-building activities, aiming for sustainability and sharing of best practices – specifically for the development of sound data governance, health management information systems, public health statistics, health-related data science and health data innovation.
	WHO will: • Support Member States' by providing technological and human capacity for health information systems, technical assistance with data collection processes supporting data analysis, and efforts to improve data quality and accurately monitor health trends, to generate reliable information, and to inform decision-making; • Advance evidence-based decision-making by focusing on sustainable health information, management systems (HMIS) and digital development systems, and in particular strengthen their capacity to collect, analyse, disseminate and use national and subnational disaggregated data to develop and monitor country policies and plans; and • Align with nationally owned monitoring and evaluation processes, structures and budgets and reduce Member States' reporting burdens and increase sustainable locally owned solutions, with clear criteria for each Member State using data.
4. WHO shall be a responsible data manager and steward	WHO will ensure that all data made available to it are processed, maintained, analyzed, disseminated and used in accordance with international standards and best practices in health data management. This includes all relevant UN data governance standards and guidance that apply to WHO pursuant to its mandate, including the standards referenced in the preamble. WHO shall ensure that all data it produces are of consistently high standards that include transparent audit trails and common reference years, as well as being timely, accurate, comparable and (where technically and legally possible) accessible.

[270] World Health Organization Data Principles, p. 4.
[271] https://www.who.int/data/principles
[272] https://apps.who.int/iris/bitstream/handle/10665/255721/9789241512657-eng.pdf;jsessionid=8A35157EF2806FF141C148928F8530AF?sequence=1
[273] https://www.who.int/docs/default-source/documents/about-us/infodisclosurepolicy.pdf?sfvrsn=c1520275_10
[274] https://www.who.int/about/who-we-are/publishing-policies/open-access

	WHO will apply international scientific data standards, maintain and strengthen partnerships with relevant stakeholders, strengthen the quality of SDG monitoring efforts and adapt to specific contexts. The following guidance is important in application of this principle: • FAIR Guiding Principles for scientific data management and stewardship' [275] • Guidelines for Accurate and Transparent Health Estimates Reporting[276] • Bridging digital divide: Digital and data governance for health[277]
5. WHO shall strive to fill public health data gaps	WHO will support Member States to fill data gaps in public health data, using empirical data collection and predictive, transparent and coherent modelling methods with proven validity.
	WHO will use transparent models and methods.[278] Member States use a range of health indicators to monitor population health and guide resource allocations but lack of data, inconsistent methods and often underdeveloped data governance and standards at all economic levels can be challenges. WHO will support Member States to generate coherent estimates.

The WHO website states that WHO is committed to strengthening the global ecosystem of public health data which includes building internal data governance capacities. The WHO data principles are intended to act as the foundations for data-related policies, plans and programme implementation.[279]

In 2018, WHO established the Data, Analytics and Delivery for Impact (DDI) Division, promoting data as a strategic asset. In 2020, WHO strengthened its data coordination and governance by instituting a two-level internal data governance system with: a strategic Data Governance Committee, chaired by the Assistant Director-General for DDI and the Deputy Director-General, and an operationally grounded, federated structure known as the Data Hub and Spoke Collaborative, chaired by the Director of Data and Analytics (DNA), DDI. This two-level governance system aims to promote ownership of data governance issues as an area of strategic importance, as well as to increase accountability and efficiency and to streamline the end-to-end processes and systems for collecting, storing, analysing, disseminating and using data. Beyond internal stakeholders, WHO will also seek advice as necessary from external expert groups such as the Reference Group on Health Statistics and the External Expert Group on Data Sharing. The website provides links to the following topics which provide more information related to data processing:[280]

- WHO Reference Group on Health Statistics;[281]

[275] https://www.go-fair.org/fair-principles/
[276] http://gather-statement.org/
[277] https://path.ent.box.com/s/1mqunwcx4evq37okfbaazcaha9vigwqm
[278] https://www.who.int/docs/default-source/world-health-data-platform/who-data-principles-10aug-(3).pdf?sfvrsn=3d89acf0_6
[279] https://www.who.int/data/principles
[280] https://www.who.int/data/principles
[281] https://www.who.int/data/who-reference-group-on-health-statistics-(rghs)

- WHO policy on the use and sharing of data collected by WHO in Member States outside the context of public health emergencies;[282]
- WHO Policy on Open Access, and;[283]
- Policy statement on data sharing by WHO in the context of public health emergencies.[284]

5.13.4 Information Disclosure Policy

The WHO Information Disclosure Policy states that WHO is committed to making information about its activities available to the public. WHO considers public access to information to be a key component of effective engagement with all stakeholders, including WHO's Member States and the public, in the fulfilment of its mandate. The Policy further states that public access to WHO information facilitates transparency and accountability and enhances trust in WHO's activities to further public health.[285]

The Information Disclosure Policy was published in 2017 to ensure that information concerning WHO's activities is made publicly available, subject to the limitations set out in the Policy. The Policy explains principles, practices and procedures and defines clear categories of information according to their status with regards to public disclosure. Information is divided into three categories in the Policy:[286]

Category 1: Publicly available information;
Category 2: Information available on request, and;
Category 3: Confidential information.

As explained in the Policy, information identified as confidential constitutes an exception to the principle of public disclosure. The exceptions to disclosure reflect what is necessary to preserve legitimate public or private (including personal privacy) interests. The following information provided in Annex 3 is considered as confidential:

- Personal information;
- Information which may compromise security and safety;
- Information concerning WHO Member States or other intergovernmental organizations;
- Information obtained or shared in confidence;
- Confidential Internal documents;
- Deliberative information;
- Privileged information;
- Financial information;
- Commercial information, and;
- Other kinds of information, which because of its nature, content or the circumstances surrounding its creation, use or communication is deemed confidential in the interests of WHO or third parties.

[282] https://www.who.int/about/who-we-are/publishing-policies/data-policy
[283] https://www.who.int/about/who-we-are/publishing-policies/open-access
[284] https://apps.who.int/iris/handle/10665/254440
[285] Information Disclosure Policy, p. 3. https://www.who.int/docs/default-source/documents/about-us/infodisclosurepolicy.pdf?sfvrsn=c1520275_10
[286] Information Disclosure Policy, p. 4.

5.13.5 Other privacy -related efforts

The WHO has a privacy policy describing WHO's policy concerning the gathering and sharing of visitors' information through the WHO web site, applying to all sites within the 'who.int' domain name.[287] WHO has further developed a policy on personal data protection, expected to be adopted in late 2021. The WHO Policy on Personal Data Protection (once adopted) is intended to be an internal policy, but it will also cover the processing of personal data provided by third parties.

In addition to the above, WHO complies with the UN Personal Data Protection and Privacy Principles and as international civil servants, all WHO staff are required to adhere to confidentiality. WHO has policies covering information security, access to information and systems, cloud computing, cyber security, application security, information classification and related security standards.[288]

WHO has a newly created working group on dissemination and capacity building and would like to institute better capacity building for its staff. The budget of this working group is small. WHO considers that the greatest challenges for it are:

- ensuring trust between Member States and WHO
- understanding what happens to data once it comes into WHO and
- overcoming siloed nature of how data is stored and used to actually enforce the policy.[289]

WHO also established a Reference Group on Health Statistics in 2013 to provide advice on population health statistics to WHO with a focus on methodological and data issues related to the measurement of mortality and cause-of-death patterns. With recent developments in global health and an increased focus on monitoring and accountability, the Reference Group was renewed in 2019 to ensure that WHO and its Member States continue to benefit from the best possible scientific and strategic advice and support in the generation, use, interpretation, and dissemination of global health statistics.[290]

The objectives of the Reference Group are not directly related to data protection or privacy but to:

- provide technical and strategic advice to ensure that WHO's practices in data processing and synthesis and producing and using population-health related statistics are evidence-based;
- strengthen collaboration between WHO and external research groups in advancing the methodological agenda for population-health estimates;
- guide WHO on strengthening data and information systems for health, and;
- promote compliance in producing population-health related statistics.

5.14 UN Global Pulse

UN Global Pulse's convening power and thought leadership has already been documented earlier as they led some of the inter-agency processes, including the UN Personal Privacy and Data Protection Principles approved by the HLCM in 2018. Some of their standalone initiatives include the following.

5.14.1 Due Diligence Tools

UN Global Pulse notes on its website that it applies a thorough two-part due diligence tool when working with prospective technology partners. The tool has been updated following the issuance of the UNDG Guidance Note on Big Data for the 2030 Agenda. The due diligence tool is part of a self-

compliance mechanism for assessing the social and corporate behaviour of a prospective partner, considering privacy and data protection practices as well as practices related to digital ethics.[291]

5.14.2 Risks, Harms and Benefits Assessment Tool

UN Global Pulse has also developed a two-phase 'Risk, Harms and Benefits Assessment Tool,' which is a data privacy, ethics and data protection compliance mechanism designed to help identify and minimize the risks of harms and maximize the positive impacts of data innovation projects. The assessment can be used at the onset of a data innovation project, or when an existing project needs to undergo changes, considering every stage of the data life cycle and, where possible, should include a diverse team of experts as well as representatives of the groups of individuals who could be potentially affected by the data use. The Tool consists of two steps the first phase being an initial assessment of potential risks for data use that should help identify whether a more comprehensive Risks, Harms and Benefits Assessment should be conducted. The second phase should be completed each time the initial assessment identified high risks of harms associated with the project. The assessment is designed primarily as a general example for internal self-regulation.[292]

5.14.3 COVID-19 Data Protection and Privacy Resources

The Global Pulse COVID-19 Data Protection and Privacy Resources website contains a selected list of data protection and privacy resources related to the COVID-19 epidemic. It includes links in the following categories:[293]

- UN resources on privacy, COVID-19 and the right to health;
- International/regional/industry initiatives to address privacy and data use for COVID-19;
- Civil society initiatives to address privacy and data use for COVID-19, and;
- Data practices to address COVID-19.

5.14.4 UN Global Pulse Principles on Data Protection and Privacy

The UN Global Pulse Principles on Data Protection and Privacy are based on the UN Principles on Personal Data Protection and Privacy, adopted by the High-level Committee on Management in 2018 and the UNSDG Guidance Note on Big Data for Achievement of the 2030 Agenda. The UN Global Pulse Principles aim to ensure proper implementation of the UN Principles on Personal Data Protection and Privacy in the practices of UN Global Pulse. Also, the UNSDG Guidance Note on Big Data for

[287] https://www.who.int/about/who-we-are/privacy-policy
[288] Dr. Azza, 26 January 2021.
[289] Dr. Azza Badr, 26 January 2021.
[290] https://www.who.int/data/who-reference-group-on-health-statistics-(rghs)
[291] https://www.unglobalpulse.org/policy/due-diligence/
[292] https://www.unglobalpulse.org/policy/risk-assessment/
[293] https://www.unglobalpulse.org/policy/covid-19-data-protection-and-privacy-resources/

Achievement of the 2030 Agenda: Data Privacy, Ethics and Protection, are used to further clarify how to apply the UN Global Pulse Principles in a 'big data' context.[294]

The 13 UN Global Pulse Principles on Data Protection and Privacy apply to all processing personal data or sensitive non-personal data as part of the activities of UN Global Pulse:

Fair and Legitimate Processing	UN Global Pulse processes data in a fair manner, in accordance with the UN global mandate and governing instruments, on the basis of any of the following: (i) the consent of the data subject; (ii) the best interests of the data subject, consistent with the UN global mandate; (iii) the United Nations global mandate and governing instruments, or; (iv) another appropriate legal basis specifically identified.
Purpose Specification	Data is processed for specified purposes, consistent with the UN global mandate and consider the balancing of relevant rights, freedoms and interests. Data is not processed in ways that are incompatible with such purposes.
Proportionality and Necessity	UN Global Pulse ensures that data that is processed is relevant, limited and adequate to what is necessary in relation to the specified purposes.
No Re-identification	De-identified data is not attempted to be re-identified knowingly and purposefully, unless there is a legitimate basis for doing so, and all reasonable efforts to prevent any illegitimate or unjustified re-identification are made.
Retention	Data is retained for the time that is necessary for the specified purposes only.
Accuracy	Data accuracy and up-dates are ensured to fulfill the specified purposes.
Confidentiality	UN Global Pulse processes data with due regard to confidentiality.
Security	Appropriate organizational, administrative, physical and technical safeguards and procedures are implemented to protect the security of the data, including against or from unauthorized or accidental access, damage, loss or other risks presented by data processing.
Data Sensitivity	Stricter standards of care while processing data that relates to vulnerable populations and persons at risk, children and young people, and when processing any other sensitive data are employed. UN Global Pulse ensures proper protection of non-personal data, that is processed in a sensitive context and that may put certain individuals or groups of individuals at risk of harms.

[294] https://www.unglobalpulse.org/policy/ungp-principles-on-data-privacy-and-protection/#:~:text=The%20Principles%20set%20out%20a,carrying%20out%20their%20mandated%20activities.&text=(iii)%20ensure%20respect%20for%20the,particular%20the%20right%20to%20privacy.

Risks, Harms, and Benefits Assessment	UN Global Pulse performs a risks, harms and benefits assessment and implements appropriate mitigation processes before any new or substantially changed data processing activity is undertaken. The impact that data processing may have not only on individuals but also on groups of individuals is taken into consideration. The risks and harms shall not be excessive in relation to the positive impact of the project.
Transparency	Data is processed with transparency to the data subjects, as appropriate and whenever possible. This includes provision of information about the processing of their personal data as well as information on how to request access, verification, rectification, and/or deletion of that personal data, insofar as the specified purpose for which data is processed is not frustrated.
Technology Collaborators and Data Transfers	Data is transferred to third parties, provided that under the circumstances, the third party affords appropriate protection for the personal data, consistent with the requirements of the relevant data privacy and data protection instruments and the United Nations' global mandate.
Accountability	UN Global Pulse designs, carries out, reports and documents its data processing activities with adequate accuracy and openness, and ensures that adequate policies and mechanisms are in place to adhere to these Principles and other relevant data privacy and data protection instruments, including the UN Principles on Personal Data Protection and Privacy.

5.15 World Bank

5.15.1 The World Bank Group Personal Data Privacy Policy

The World Bank Group's Personal Data Privacy Policy was published in May 2018. The WBG considers that protecting personal data is not only about managing risks but also about corporate social responsibility and about maintaining trust. Putting in place safeguards to protect personal data is the right thing for any responsible organization to do.[295]

Personal data plays a key role in the Group's operational and transaction work, procurement, household surveys, safeguards, and integrity and compliance functions. At the most basic level, improved personal data management will help protect the people most vital to the Bank Group's mission: the staff at the headquarters and in offices around the world and the people who benefit from the Bank Group's development projects. The Bank Group has over 15,000 clients and partners based in the EU who are subject to application of the GDPR.[296]

he WBG's Personal Data Privacy Policy sets forth Principles governing the Processing of Personal Data by WBG Institutions. The WBG Institutions are International Bank for Reconstruction and Development, International Development Association, the International Centre for Settlement of Investment Disputes, the International Finance Corporation and Multilateral Investment Guarantee Agency. The Policy has been rolled out over the course of a few years, with supporting directives, procedures and guidelines, strengthened IT controls, improved security architectures, and staff training tailored to each WBG institution. The programmes will be designed to maintain client/partner trust by demonstrating that each institution has a mature data protection regime in place.[297]

The Policy is intended to ensure consistent practices, aligned with recognized international standards, for the Processing of Personal Data by WBG Institutions. The Policy states that privacy laws and regulations do not apply directly to the institutions of the Bank Group because of their privileges and immunities as international treaty-based organizations, as stated in Section VI of the Policy. However, if the Bank Group cannot demonstrate to its clients and partners worldwide that it takes the protection of personal data seriously, its ability to do business with these counterparties is at risk. Therefore, there is an imminent need for the Bank Group to apply privacy rules.[298]

Section III of the Policy sets the following seven Principles that apply to all Processing of Personal Data by WBG institutions:

Legitimate, Fair and Transparent Processing	Personal data shall be processed for legitimate purposes and in a fair and transparent manner in accordance with this Policy. Legitimate purposes for processing of personal data mean any purpose: • carried out with the consent of the individual whose personal data is being processed; • in the vital or best interest of the individual whose personal data is being processed, or of another person; • necessary for the performance of a contract or compliance with a binding obligation or undertaking, or;

	• consistent with, or reasonably necessary to enable a WBG institution to carry out, its mission, mandate or purpose as an international organization established by its member countries.
Purpose Limitation and Data Minimization	Personal data shall be collected for one or more specific and legitimate purpose(s) and not further processed in a manner that is incompatible with the original purpose(s) for which it was collected. Further processing for archiving purposes, research, or statistical purposes shall not be considered incompatible with the original purpose. In amount and type, personal data collected shall be necessary for and proportionate to the legitimate purpose(s) for which they are processed.
Data Accuracy	Personal data shall be recorded as accurately as possible and, where necessary, updated to ensure it fulfills the legitimate purpose(s) for which it is processed.
Storage Limitation	Personal data shall be kept in a form which permits identification of individuals only so long as necessary for the fulfillment of the purposes for which it was collected or for compatible further processing in accordance with this Policy.
Security	Personal data shall be protected by appropriate technical and organizational safeguards against unauthorized processing and against accidental loss, destruction or damage.
Transfer of Personal Data	Personal data shall only be transferred to third parties for legitimate purposes and with appropriate regard for the protection of personal data.
Accountability and Review	Each WBG institution shall adopt mechanism(s) to: • oversee compliance with the Policy, and; • provide individuals with a method, subject to reasonable limitations and conditions, to request information regarding the individual's personal data processed by such WBG Institution and seek redress if the individual reasonably believes that the individual's personal data has been processed in violation of this Policy.

The Policy explicitly states that the privileges and immunities of the WBG institutions are specifically reserved and that processing of personal data in accordance with the Policy is without prejudice to the privileges and immunities. This Policy shall be implemented by each WBG institution through directives and guidance tailored to each institution's specific operations. Other related documents include:

- IBRD Access to Information Policy
- IFC Access to Information Policy

[295] http://documents1.worldbank.org/curated/en/466121527794054484/pdf/Privacy-Board-Paper-050318-vF-05042018.pdf p. 4
[296] http://documents1.worldbank.org/curated/en/466121527794054484/pdf/Privacy-Board-Paper-050318-vF-05042018.pdf p. 5
[297] World Bank Group Personal Data Privacy Policy, p. 13. http://documents1.worldbank.org/curated/en/466121527794054484/pdf/Privacy-Board-Paper-050318-vF-05042018.pdf
[298] WBG Personal Data Privacy Policy, p. 6.

- MIGA Access to Information Policy
- Integrity Vice Presidency Policy on Disclosure of Information, and
- Independent Evaluation Group Access to Information Policy.[299]

5.15.2 Identification for Development (ID4D)

The World Bank Group's ID4D Initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals and in particular Target 16.9: "By 2030, provide legal identity for all, including birth registration", and in making progress towards dozens of other targets such as poverty elimination, reduced inequalities, gender equality and women's empowerment, safe and orderly migration, universal health coverage, and financial inclusion. Technical assistance relating to development of legal and regulatory framework, including guidance on data protection and privacy requirements, are provided to governments within this initiative. In response to a country's request, the ID4D Initiative conducts assessments of its identity ecosystem using the Guidelines for ID4D Diagnostics. ID4D has implemented more than 30 country diagnostics facilitating engagement and dialogue within countries.[300]

An ID4D Diagnostic involves an evaluation of a country's identity ecosystem according to international best practices and the Principles on Identification for Sustainable Development. An identification system consists of the databases, processes, technology, credentials, and legal frameworks associated with the capture, management, and use of personal data for a general or specific purpose.[301]

Data protection and privacy plays an important role in the identification systems. To maximize the potential for sustainable development, identification systems should have robust identity databases and credentials, and provide services that are trusted, integrated with other systems, and responsive to user demand. Sufficient administrative and technical capacity, appropriate technical design choices, and careful attention to user privacy and data protection are required.[302] According to the ID4D Guidelines management of personal data is a core activity of identity providers, with broad implications for overall system quality, utility, and privacy protection.[303]

The ID4D programme was the convener of the Principles on Identification for Sustainable Development, which a number of UN agencies, funds and programmes (including UNDP) have endorsed.

- Principle 3 relates to data protection. The robustness of identification systems, including the uniqueness, accuracy, and security of individual identities, depends on the quality of information collected during the registration, the frequency of updating, the strength of

[299] WBG Personal Data Privacy Policy, p. 20-21.
[300] ID4D Program Brochure, p. 1. https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2019-10/ID4D%20Program%20Brochure%2010152019.pdf
[301] Guidelines for ID4D Diagnostics, p. 3. http://documents1.worldbank.org/curated/en/370121518449921710/Guidelines-for-ID4D-Diagnostics.pdf
[302] Guidelines for ID4D Diagnostics, p. 13.
[303] Guidelines for ID4D Diagnostics, p. 22.

validation processes, and the procedures for storing and managing personal data. Systems that are initially strong may lose robustness if the identity provider does not have a method for frequently and reliably updating identity attributes – such as address, occupation, and marital status – or cleaning the database to remove deceased persons. Weak data storage practices, such as paper registers and insufficient backup, also compromise system robustness.[304]

- Principle 6 includes 'Protecting user privacy and control through system design.' The ID4D Guidelines state that the technology and procedures for data collection, validation, storage, and updating can either protect or infringe user privacy.[305] Part 4 of the Guidelines assesses the governance of identification systems focusing on the degree to which the county's legal framework builds trust and protects user privacy and rights with regard to identification. According to the Guidelines, identification systems should be built on a legal and operational foundation of trust and accountability between government agencies, international organizations, private sector actors and individuals. To this end, the ID4D Diagnostic includes a proposal for analysis of governance frameworks across all identification systems which comprises existing and draft country laws, codes, regulations, and agency practices related to:[306]

    - the administration and authority of national ID agencies, civil registers, and other identity providers;
    - the collection, storage, and use of personal data, both analog and digital;
    - conferring or proving citizenship or legal status through identification systems;
    - user privacy and data protection;
    - accountability and oversight, both between identity providers and other government agencies, and between identity providers and users.

- Principle 8 includes safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework. According to the ID4D Guidelines, identification systems should be underpinned by comprehensive legal frameworks and practices that promote trust in the system while stimulating competition and investment. This includes ensuring the protection of individual data, privacy and user rights. Individuals should have genuine choice and control over the use of their data, including the ability to:
    1. selectively disclose only those attributes required for a particular transaction;
    2. easily correct inaccurate data free of charge, initially through administrative (rather than judicial) processes, and;

[304] Guidelines for ID4D Diagnostics, p. 16.
[305] Guidelines for ID4D Diagnostics, p. 17.
[306] Guidelines for ID4D Diagnostics, p. 26.

3. obtain a copy of their personal records, as well as information on who has accessed them.

In addition, personal information should not be used for unauthorized surveillance or profiling by governments or third parties, or secondary, or used for unconnected purposes without consent (unless otherwise required under the law). Legal frameworks and policies related to data sharing and usage should be clearly and publicly documented and be updated to reflect the digital age.

- Principle 9 includes establishing clear institutional mandates and accountability and encompasses the creation of a harmonized, robust identification system with wide coverage and an overarching legal and procedural framework that provides transparent and comprehensive institutional mandates and accountability. The role of each identity provider should be clear and publicly available, as should responsibilities within each institution. The ID4D Guidelines state that identity providers should establish memoranda of understanding (MOUs) with other agencies for the exchange and use of data and for authentication and verification services.[307]

- Principle 10 includes enforcing legal and trust frameworks though independent oversight and adjudication of grievances. The ID4D Guidelines state that countries should have independent oversight bodies for ensuring compliance with legal and policy frameworks related to the collection and management of personal data. Such entities should be empowered to ensure that identity providers adhere to their mandates and responsibilities, respond to potential data breaches, and adjudicate and redress disputes over the use of personal data that are not resolved through administrative processes.[308]

6 SELECTED DATA PROTECTION AND PRIVACY INSTRUMENTS OUTSIDE THE UN SYSTEM

6.1 African Union Convention on Cyber Security and Personal Data Protection

The AU Convention on Cybersecurity and Personal Data Protection was adopted by AU Heads of States and Governments in June 2014. The United Nations Economic Commission for Africa helped create the

[307] Guidelines for ID4D Diagnostics, p. 26.
[308] Guidelines for ID4D Diagnostics, p. 27.

Convention together with the African Union. The Convention is based on the continent's needs and adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection. UNECA has supported several African countries [309] in the implementation of the Convention as well as to develop sound regulation to safeguard privacy and personal data.[310]

The provisions regarding Personal Data Protection are in Chapter II of the Convention. Chapter I of the Convention relates to electronic transactions, Chapter III relates to promoting cyber security and combating cybercrime, and Chapter IV includes the final provisions. The objective of the Convention with respect to personal data is that each State Party commits itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data. The mechanism so established shall ensure that any form of data processing respects the fundamental freedoms and rights of natural persons while recognizing the prerogatives of the State, the rights of local communities and the purposes for which the businesses were established.[311]

According to Article 9, the Convention applies to any collection, processing, transmission, storage or use of personal data by a natural person, the State, local communities, and public or private corporate bodies. It is not applicable to data processing undertaken by a natural person within the exclusive context of her/his personal or household activities and to temporary copies produced within the context of technical activities for transmission and access to a digital network with a view to automatic, intermediate and temporary storage of data and for the sole purpose of offering other beneficiaries the best possible access to the information so transmitted.

Article 10 of the Convention requires an authorization by the national protection authority for processing of personal data involving genetic information and health research and other such sensitive data. According to Article 11 each State Party shall establish an independent authority in charge of ensuring that the processing of personal data is conducted in accordance with the Convention.

Article 13 includes the following basic principles governing the processing of personal data:

Consent and legitimacy	Processing of personal data shall be deemed to be legitimate where the data subject has given her/his consent. This requirement of consent may however be waived where the processing is necessary for matters as mentioned in the article.
Lawfulness and fairness	The collection, recording, processing, storage and transmission of personal data shall be undertaken lawfully, fairly and non-fraudulently.

[309] These countries include Burundi, Cameroon, Comoros, Rep of Congo, DR Congo, Djibouti, Ethiopia, The Gambia, Ghana, Guinea, Kenya, Niger, Rwanda, Senegal, Seychelles, South Africa, Togo, Tunisia, Zambia, and Zimbabwe
[310] https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
[311] Article 8 of the Convention

Purpose, relevance and storage	a) Data collection shall be undertaken for explicit, legitimate purposes, and not further processed incompatible with those purposes. b) Data collection shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and processed. c) Data shall be kept for no longer than is necessary for the purposes for which the data were collected or further processed. d) Beyond the required period, data may be stored only for the specific needs of data processing undertaken for historical, statistical or research purposes under the law.
Accuracy	Data collected shall be accurate and, where necessary, kept updated. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or further processed, are erased or rectified.
Transparency	The principle of transparency requires mandatory disclosure of information on personal data by the data controller.
Confidentiality and security	a) Personal data shall be processed confidentially, in particular where the processing involves transmission of the data over a network. b) Where processing is undertaken on behalf of a controller, the latter shall choose a processor providing sufficient guarantees. It is incumbent on the controller and processor to ensure compliance with the security measures defined in the Convention.
Processing of sensitive data	State Parties shall undertake to prohibit any data collection and processing revealing racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject.

The Convention also includes provisions on data subjects' rights, such as right to information, right of access, right to object and right of rectification or erasure. Obligations of the Personal Data Controller are stated in section V and include confidentiality, security, storage and sustainability obligations to the controller. The sustainability obligations mean that the controller takes all appropriate measures to ensure that processed personal data can be utilized regardless of the technical device employed in the process. Technological changes shall not constitute an obstacle to the data use.[312] According to Article 36 the Convention shall enter into force 30 days after the receipt of the 15th instrument of ratification. As of August 2021, only nine of the AU Member States have ratified the Convention.[313]

6.2 Council of Europe

6.2.1 Treaty 108+

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, i.e., Treaty No.108, which opened for signature in 1981, is the first binding international instrument which

[312] The Convention, p. 24.
[313] https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transborder flows of personal data.

In addition to providing guarantees in relation to the collection and processing of personal data, it prohibits the processing of sensitive data in the absence of proper legal safeguards. The Convention also establishes the individual's right to know that information is stored on her/him and, if necessary, to have it corrected. The Convention also imposes some restrictions on transborder flows of personal data.

With new challenges to human rights and fundamental freedoms, notably to the right to private life, arising every day, it appeared clear that the Convention should be modernised in order to better address emerging privacy challenges resulting from the increasing use of new information and communication technologies, the globalisation of processing operations and the ever-greater flows of personal data, and, at the same time, to strengthen the Convention's evaluation and follow-up mechanism, and to bring it into line with the General Data Protection Regulation. The Treaty modernization took place in 2018 and it is since called Treaty 108+.[314]

The modernization concerned the following Articles of the Treaty:

- Object and purpose of the Convention (Article 1)
- Definitions and scope of application (Articles 2 and 3)
- Duties of the parties (Article 4)
- Legitimacy of data processing and quality of data (Article 5)
- Sensitive data (Article 6)
- Data security (Article 7)
- Transparency of processing (Article 8)
- Rights of the data subject (Article 9)
- Additional obligations (Article 10)
- Exceptions and Restrictions (Article 11)
- Transborder flows of personal data (Article 14)
- Supervisory authorities (Article 15)
- Forms of co-operation (Article 17)
- Convention Committee (Articles 22, 23 and 24).[315]

The Treaty sets out the following basic principles for the protection of personal data:

Duties of the parties	Each Party shall take the necessary measures in its law to give effect to the provisions of this Convention and secure their effective application

[314] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (*), p. 1-2. https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a

[315] The modernised Convention 108: novelties in a nutshell https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8

Legitimacy of data processing and quality of data	Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake. Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law. Personal data undergoing processing shall be processed lawfully. Personal data undergoing processing shall be: • processed fairly and in a transparent manner; • collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes; • adequate, relevant and not excessive in relation to the purposes for which they are processed; • adequate, relevant and not excessive in relation to the purposes for which they are processed; • accurate and, where necessary, kept up to date, and; • preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.
Sensitive data	The processing of sensitive data shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.
Data security	Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorized access to, destruction, loss, use, modification or disclosure of personal data.
Transparency of processing	Each Party shall provide that the controller informs the data subjects of his or her identity and habitual residence or establishment, the legal basis and the purposes of the intended processing, the categories of personal data processed, the recipients or categories of recipients of the personal data, if any, and the means of exercising the rights, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.
Rights of the data subject	Every individual shall have a right: - not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration; - to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her; - to object; - of rectification or erasure; - to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;

	- to remedy, and; - to assistance of a supervisory authority within the meaning of Article 15, in exercising her or his rights under this Convention.
Additional obligations	Each Party shall provide that controllers and, where applicable, processors, take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate that the data processing under their control follows the provisions of this Convention.
Exceptions and restrictions	No exception shall be allowed except in certain cases when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for: a. the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest, and; b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.
Sanctions and remedies	Each Party undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of the Convention.
Extended protection	None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in the Convention.

6.2.2 Budapest Convention

The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention, is the only binding international instrument on cybercrime serving as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State Parties to the treaty. The Budapest Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.[316]

The Budapest Convention is not a data protection instrument. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation, and to foster international co-operation. The Convention entered into force 1 July 2004.[317]

[316] https://www.coe.int/en/web/cybercrime/the-budapest-convention
[317] https://rm.coe.int/1680081561

6.3 European Union

6.3.1 The data protection package

The 'data protection package', including the General Data Protection Regulation and the Law Enforcement Directive (adopted in May 2016), aims at making Europe fit for the digital age.

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, i.e., the GDPR, may be considered as the world reference in the area of protection of personal data currently. It does not apply to the processing of personal data by the European Commission or other EU institutions but in the context of the activities of an establishment of other controllers or processors in the European Union, regardless of whether the processing takes place in the Union or not. It also applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services or the monitoring of their behaviour as far as their behaviour takes place within the Union.

The 25 May 2018 entry into force of the GDPR is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market.[318] Article 5 of the GDPR provides principles relating to processing of personal data.

PRINCIPLE	Personal Data shall be:
Lawfulness, fairness and transparency	• processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose limitation	• collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.
Data minimisation	• adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	• accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
Storage limitation	• kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the

[318] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

	appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.
Integrity and confidentiality	• processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
Accountability	• The controller shall be responsible for and be able to demonstrate compliance with the above.

Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (and repealing Council Framework Decision 2008/977/JHA) was adopted in parallel with the GDPR. The Data Protection Law Enforcement Directive (LED) applies to the processing of personal data by competent authorities for the purposes set above. However, it does not apply to the processing of personal data in the course of activity which falls outside the scope of Union law or by the Union institutions, bodies, offices and agencies. Processing carried out to ensure state security or national defense does not fall within the scope of the European Union and remains governed by the national laws of the EU Member States. The LED entered into force on 6 May 2016 and was to be transposed into the national law by the EU countries by 6 May 2018. The directive protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities for law enforcement purposes. It will, in particular, ensure that the personal data of victims, witnesses, and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism.

The rules for the processing of personal data in the LED are largely consistent with the provisions laid down in the GDPR. Article 4 establishes the data protection principles.

PRINCIPLE	Personal Data shall be:
Lawfulness and fairness	• processed lawfully and fairly.
Purpose limitation	• collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes. • Processing for other purposes than those for which the personal data are collected shall be permitted in so far as: • the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law, and; • processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.

Data minimisation	• adequate, relevant and not excessive in relation to the purposes for which they are processed.
Accuracy	• accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
Storage limitation	• kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed.
Integrity and confidentiality	• processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Accountability	• The controller shall be responsible for and be able to demonstrate compliance with the above.

While the GDPR requires the processing of personal data to be transparent, Article 4 of the LED does not require it. However, Recital 26 mentions that any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. Further it is stated that the law-enforcement authorities are not prevented from carrying out activities, such as covert investigations or video surveillance, that can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned.[319]

For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected.[320]

Article 5 of the Directive requires Member States to provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Article 6 relates to different categories of data subjects stating that Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:

- persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
- persons convicted of a criminal offence;

[319] Recital 26 of the LED.
[320] Recital 27 of the LED.

- victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence, and;
- other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the above persons.

Rights of the data subject are provided for in Chapter III. As with the GDPR, the LED includes a provision in data protection by design and by default. Article 25 requires logs to be kept for automated processing operations such as collection, alteration, consultation, disclosure (including transfers), combination and erasure of personal data. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such data. The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the data, and for criminal proceedings, and made available to the supervisory authority on request.

While in the GDPR the processing of personal data is substantially dependent upon the consent of the personal data subject, consent cannot be used to the same extent as a legal basis for data processing in the activities of judicial authorities. In accordance with the principle of legality, such processing should be carried out solely in connection with the fulfilment of specific tasks provided for by law. The LED includes a broader understanding of the principle of purpose limitation of data processing. Differences exist also in relation to information to be made available or given to the data subject as well as to access rights and limitations of the data subject.

Article 6 of the Directive urged Member States to differentiate the categories of personal data processed as between different categories of data subjects. The concrete implementation of this provision remains within the competence of Member States.

6.3.2 Regulation 2018/1725

The applicable data protection instrument for the European Commission is Regulation 2018/1725 of October 2018 applying to the processing of personal data by all Union institutions and bodies (the GDPR not applying to the processing of personal data by the European Union institutions).[321]

In line with the GDPR, the Regulation adopts a principle-based approach ensuring that EU institutions and bodies provide transparent and easily accessible information on how personal data is used and foresees clear mechanisms for individuals to exercise their rights. The Regulation also confirms, clarifies and enhances the role of data protection officers within each EU institution, and of the European Data Protection Supervisor.[322]

[321] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1725

[322] https://edps.europa.eu/data-protection/our-work/subjects/regulation-20181725_en

Principles relating to processing of personal data in Article 4 of the Regulation 2018/1725 are similar to those in Article 5 of the GDPR.

PRINCIPLE	Personal Data shall be:
Lawfulness, fairness and transparency	• processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose limitation	• collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 13, not be considered to be incompatible with the initial purposes.
Data minimisation	• adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	• accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
Storage limitation	• kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 13 subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject
Integrity and confidentiality	• processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
Accountability	• The controller shall be responsible for, and be able to demonstrate compliance with, the above.

The Regulation 2018/1725 aims to ensure that EU institutions and bodies provide transparent and easily accessible information on how personal data is used, as well as foresee clear mechanisms for individuals to exercise their rights. In accordance with Article 31, each controller of personal data shall maintain a record of processing activities under its responsibility. The records replace the previous system of notifications. Register of the Data Protection Officer of the European Commission is available for public consultation and it includes records of more than 800 processing activities.[323]

[323] https://ec.europa.eu/dpo-register/

6.3.3 Privacy and electronic communications

The Directive 2002/58 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, revised in 2009, set out rules on the security of personal data in electronic communication networks. Article 4 of the revised version provides that in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.[324] A proposal for a Regulation on Privacy and Electronic Communications was published in 2017, aiming to update the Directive 2002/58. The Regulation is to lay down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data. The Regulation is to apply to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.[325]

Unlike the GDPR or Regulation 2018/1725, the approach of the proposal for e-Privacy regulation is not principle-based. Article 5 in Chapter II of the Proposal provides for confidentiality of electronic communications data stating that electronic communications data shall be confidential and that any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by the Regulation.

Article 6 provides for permitted processing of electronic communications data. Electronic communications data may be processed if it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose or it is necessary to maintain or restore the security of electronic communications networks and services or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose. Different rules apply regarding electronic communications metadata and electronic communications content.

Chapter III of the Proposal establishes the rules related to the rights to control electronic communications. Article 16 concerns unsolicited communications and states that natural or legal persons may use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons that have given their consent. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent.

[324] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
[325] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

Chapter IV relates to independent supervisory authorities and enforcement and reference is made to the authorities stated in the GDPR. In Chapter V (remedies, liability and right to compensation and penalties), reference is equally made to the provisions of the GDPR Chapter VII of the GDPR applying to infringements of the e-Privacy Regulation. In addition, in accordance with Article 23 of the Proposal, administrative fines up to EUR10,000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year (whichever is higher) apply to infringements of the following provisions:

a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;
b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;
c) the obligations of the providers of publicly available directories pursuant to Article 15, and;
d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.

6.3.4 Commission Decision (EU) 2020/969

Commission Decision (EU) 2020/969 of 3 July 2020 lays down implementing rules concerning the Data Protection Officer, restrictions of data subjects' rights and the application of Regulation (EU) 2018/1725 (and repeals the previous such Commission Decision (2008/597/EC). Its first chapter includes general provisions, the second one providing for a data protection officer and data protection coordinator.

Article 5 includes the tasks and duties of the DPO, and Article 6 its powers in performing the DPO tasks. The DPO shall contribute to creating a culture of protection of personal data within the Commission based on risk assessment and accountability. Article 7 provides for the Data Protection Coordinators, their competence, tasks etc.[326]

6.3.5 Practical Guide on Contract Procedures for European Union External Action

The Practical Guide on Contract Procedures for European Union External Action provides contracting authorities, on the one hand, and tenderers, candidates, applicants and contractors, on the other hand, with practical assistance in preparing and implementing procurement and granting contracts in the field of external action. Contracts under procurement and grants are awarded according to strict data protection and other rules. [327]

The beneficiaries of European Union financed grant contracts must process personal data under the Agreement in compliance with applicable EU and national law on data protection.[328] The Practical Guide includes rules and practices on service contracts, supply contracts, work contracts and grants.

Regarding service contracts for external actions financed by the European Union or by the European Development Fund, Article 8 of the Annex 1 to the Practical Guide states that the contractor and its staff shall respect human rights, data protection rules and the environmental legislation applicable in the

[326] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2020:213:FULL&from=EN
[327] https://ec.europa.eu/europeaid/prag/document.do?nodeNumber=1
[328] https://ec.europa.eu/europeaid/prag/annexes.do?annexName=E3h2&lang=en

country where the services are to be rendered and internationally agreed core labour standards. Article 36 states that European Commission may terminate a contract due to a breach of data protection obligations. Article 42 regulates processing of personal data by the contractors and imposes how they should process personal data on the behalf of the European Commission. Article 42.1 states that any personal data included in or relating to the contract, including its implementation, shall be processed in accordance with Regulation 2018/1725. Such data shall be processed solely for the purposes of the implementation, management and monitoring of the contract by the data controller. [329]

6.3.6 PNR Directive

Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime defines the responsibilities of EU countries regarding the collection of PNR data, requiring them to:

- establish specific entities responsible for the collection, storage, and processing of PNR data - the so-called passenger information units (PIUs), and;
- adopt a list of competent authorities entitled to request or receive PNR data.[330]

The Directive applies to flights arriving from third countries to the EU, but EU countries can decide to apply them to intra-EU flights. It provides data protection safeguards for the PNR data, stating that e.g.:

- sensitive data must not be processed;
- data must be depersonalised after 6 months;
- data may be re-personalised only under strict conditions;
- data must be deleted after 5 years;
- a data protection officer is appointed in each PIU, and;
- an independent national supervisory authority must oversee the processing activities.[331]

Article 12 of the PNR Directive requires Member States to ensure that the PNR data provided by the air carriers to the PIU are retained in a database at the PIU for a period of five years after their transfer to the PIU of the Member State on whose territory the flight is landing or departing. Upon expiry of a period of six months after the transfer of the PNR data referred to above all PNR data shall be depersonalised through masking out the data elements which could serve to directly identify the passenger to whom the PNR data relate.

6.3.7 The Digital Services Act package

The Digital Services Act and Digital Markets Act encompass a single set of new rules applicable across the whole EU to create a safer and more open digital space. The Acts target the creation of a safer digital space in which the fundamental rights of all users of digital services are protected and the establishment of a level playing field to foster innovation, growth, and competitiveness, both in the European Single

[329] https://ec.europa.eu/europeaid/prag/annexes.do?annexName=B8d&lang=en

[330] https://eur-lex.europa.eu/eli/dir/2016/681/oj

[331] https://ec.europa.eu/home-affairs/what-we-do/policies/law-enforcement-cooperation/information-exchange/pnr_en

Market and globally.[332] Both Acts complement but do not amend the European data protection laws. The European Data Protection Supervisor considers that the Proposal will clearly have an impact on processing of personal data and considers it necessary to ensure complementarity in the supervision and oversight of online platforms and other providers of hosting services.[333]

6.4 International Committee of the Red Cross

6.4.1 ICRC Rules on Personal Data Protection

To safeguard the neutrality, impartiality and independence of the ICRC's action (and in keeping with the exclusively humanitarian nature of such action), ICRC Personal Data Processing is governed exclusively by the ICRC Rules on Personal Data Protection and independently supervised by the ICRC Data Protection Office. Remedies are ensured through the ICRC Data Protection Independent Control Commission.

The ICRC Rules on Personal Data Protection[334] include provisions in the following six main categories: basic principles, rights of data subjects, ICRC commitments, data transfers, implementation and review and updates. They include the following six Basic Principles:

Lawfulness and fair processing	The ICRC shall process personal data only if there is a lawful basis for doing so in these rules (Article 1).
Transparent processing	Data processing must be transparent to the data subjects involved. Data subjects must be given a certain minimum amount of information about the processing (Article 2).
	Minimum information about data processing must be provided to data subjects (Article 7).
Processing for specific purposes	When collecting data, the ICRC staff in charge determines the specific and legitimate purpose/s for which data are processed; the data are then processed only for those purposes.
	The ICRC may also process data in connection with any other activity necessary to carry out its mandate (Article 3).
Adequate and relevant data	The data handled by the ICRC must be adequate and relevant to the purposes for which they are collected and processed (Article 4).
Data quality	Personal data must be as accurate and up to date as possible (Article 5).
Retention, deletion and archiving	In order to ensure that data are not kept longer than necessary, a minimum retention period is set (Article 6).
	Personal data must be deleted when:
	a) they are no longer necessary for the purposes for which they were collected or otherwise further processed;
	b) the data subjects withdraw their consent for processing;

[332] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[333]Opinion 1/2021 on the Proposal for a Digital Services Act, EDPS, 10/02/2021, p. 3. https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf
[334] Available through the link https://shop.icrc.org/icrc-rules-on-personal-data-protection-pdf-en

	c) the data subjects object to the processing and their objections are upheld by the ICRC staff in charge or the ICRC Data Protection Independent Control Commission (Data Protection Commission);
	d) these rules otherwise provide for deletion.

The rules are intended to ensure that the ICRC can carry out its mandate under international humanitarian law and the Statutes of the International Red Cross and Red Crescent Movement in a manner consistent with internationally recognized standards for protecting personal data. The Rules are though intended for internal use – to tell how ICRC does and should process personal data.

6.4.2 Handbook on data protection in humanitarian action

The Handbook on data protection in humanitarian action was published as part of the Brussels Privacy Hub and ICRC's Data Protection in Humanitarian Action project. It is aimed at the staff of humanitarian organizations involved in processing personal data as part of humanitarian operations, particularly those in charge of advising on and applying data protection standards. [335]

The Handbook states that personal data protection is of fundamental importance for humanitarian organizations and an integral part of protecting the life, integrity and dignity of their beneficiaries and builds on existing guidelines, procedures and practices established in humanitarian action in the most volatile environments (and for the benefit of the most vulnerable victims of humanitarian emergencies). The Handbook seeks to help humanitarian organizations comply with personal data protection standards, by raising awareness and providing specific guidance on the interpretation of data protection principles in the context of humanitarian action, particularly when new technologies are employed. [336]

IOM was part of the Advisory Group and assisted in the drafting of the ICRC Handbook. The Handbook provides guidance on the application of data protection principles to the very unique specificities of humanitarian action, and then describes this guidance according to the specific features of new technologies that are of particular relevance for humanitarian action. Humanitarian organizations collect and process the personal data of individuals affected by humanitarian emergencies in order to perform humanitarian activities. The Handbook provides recommended minimum standards for the processing of personal data. Humanitarian organizations may provide for stricter data protection requirements, should they deem it appropriate or be subject to stricter laws at the domestic or regional level.[337]

Part I of the Handbook includes general considerations, in particular basic principles of data protection, as well as information on legal bases for personal data processing, international data sharing and data protection impact assessments. Part II relates to specific processing situations and technologies. The basic principles of data protection include the following data protection principles:

[335] The Handbook, p. 10.
[336] P. 13.
[337] P. 23-28.

THE PRINCIPLE OF THE FAIRNESS AND LAWFULNESS OF PROCESSING	Personal data should be processed fairly and lawfully. The lawfulness of the processing requires a legal basis for processing operations to take place, as detailed in Chapter 3: Legal bases for Personal Data Processing. The other crucial component of fairness of the processing is transparency.
THE PURPOSE LIMITATION PRINCIPLE	At the time of collecting data, the humanitarian organization should determine and set out the specific purpose/s for which data are processed. The specific purposes should be explicit and legitimate. In particular, the specific purpose/s that may be of relevance in a humanitarian context may include, for example: • providing humanitarian assistance and/or services to affected populations to sustain livelihoods, or; • restoring family links between people separated due to humanitarian emergencies.
THE PRINCIPLE OF PROPORTIONALITY	The data handled by humanitarian organizations should be adequate, relevant and not excessive for the purposes for which they are collected and processed. This requires, in particular, ensuring that only the personal data that are necessary to achieve the purposes (fixed in advance) are collected and further processed and that the period for which the data are stored, before being anonymized or deleted, is limited to the minimum necessary.
THE PRINCIPLE OF DATA MINIMIZATION	Data minimization requires limiting personal data processing to the minimum amount and extent necessary. Personal data should be deleted when they are no longer necessary for the purposes of the initial collection or for compatible further processing. Data must also be deleted when data subjects have withdrawn their consent for processing or justifiably object to the processing.
THE PRINCIPLE OF DATA QUALITY	Personal data should be as accurate and up to date as possible. Every reasonable step should be taken to ensure that inaccurate personal data are deleted or corrected without undue delay, considering the purposes for which they are processed.
THE PRINCIPLE OF ACCOUNTABILITY	The principle of accountability is premised on the responsibility of data controllers to comply with the above principles and the requirement to be in a position to demonstrate that adequate and proportionate measures have been undertaken within their respective organizations to ensure compliance with them. The following measures are strongly recommended in order to allow humanitarian organizations to meet data protection requirements: • drafting personal data processing policies (including processing security policies); • keeping internal records of data processing activities; • creating an independent body to oversee the implementation of the applicable data protection rules, such as a data protection office, and appointing a data protection officer; • implementing data protection training programmes for all staff; • performing data protection impact assessments (DPIAs);

	• registering with the competent authorities (including data protection authorities), if legally required and not incompatible with the principle of "do no harm."

6.4.3 Policy on the Processing of Biometric Data by the ICRC

The Policy on the Processing of Biometric Data by the ICRC was adopted in August 2019. It applies to all biometric data processing by ICRC staff and programmes in accordance with the official duties and activities of National Society staff authorised to process biometric data on behalf of the ICRC by the Staff in Charge of a particular ICRC programme. The purpose of the Policy on the Processing of Biometric Data by the ICRC is to ensure that the processing of biometric data by the ICRC takes place in accordance with the principle of "do no harm," the humanitarian imperative, the ICRC protection mandate and the ICRC Rules on Personal Data Protection. It also seeks to ensure that the Rules are applied in a manner that considers the specific features of biometric data and the risks associated with their processing. [338]

The ICRC has long been using biometrics to support the implementation of its mandate in limited use cases, for example in respect to forensics and the restoration of family links. As new technology provides new opportunities for the organization to use biometrics in different contexts, a Biometrics Policy was designed to facilitate their responsible use and address the data protection challenges this poses.[339]

Biometric data is widely recognized as sensitive personal data because once it has been collected, if retained, it creates a permanently identifiable record of an individual. For ICRC beneficiaries this can be problematic because they may not want to be identifiable forever – on the contrary – particularly if there is a risk that data may be leaked or subject to unauthorized access by third parties. For the ICRC, the protection of personal data whose disclosure could put its beneficiaries at risk, or otherwise be used for purposes other than those for which it was collected, is an integral means of preserving its neutrality, impartiality, and independence, as well as the exclusively humanitarian nature of its work.[340]

The Policy applies to all biometric data processed by ICRC staff and programmes in accordance with their official duties and activities, as well as to personal data processed by the ICRC for the purpose of creating a biometric 'template' or 'profile' regardless of format. As such it includes biological reference samples, images used for digital matching, and the 'converted' data created for the purposes of comparison.[341]

Core elements of the Policy also apply to situations in which the ICRC may use biometric data processed by partners or service providers for the purposes of authenticating or verifying the identity of its beneficiaries, even if that data is not actually processed by the ICRC.[342]

Chapter 4 provides for roles and responsibilities when processing biometric data. The legitimate bases for the processing of biometric data by the ICRC are provided in Chapter 5 and specified purposes of the

[338] https://www.icrc.org/en/document/icrc-biometrics-policy
[339] https://www.icrc.org/en/document/icrc-biometrics-policy
[340] The ICRC biometrics policy | International Committee of the Red Cross
[341] Chapter 2.1 of the Policy
[342] Chapters 2.2 and 2.3 of the Policy

processing of biometric data by the ICRC in Chapter 6. The Policy includes information, inter alia, for the following subjects:

- Authorised biometric data types and processing techniques;
- Adequacy, relevance and minimisation of biometric data;
- Non-mandatory nature of biometric processing by the ICRC;
- Data Protection Impact Assessment for processing operations involving biometric data;
- Data protection by design and default and security of biometric data processing;
- Transfer of biometric data to third parties;
- Data breaches;
- Retention of biometric data by the ICRC;
- Transparency of biometric data processing by the ICRC;
- Rights of the data subject.

6.4.4 Code of Conduct on Data Protection of the Family Links Network

The Code of Conduct on Data Protection of International Red Cross and Red Crescent Movement Family Links Network was published 2015.[343] It sets out the minimum principles, commitments, and procedures that the ICRC, National Societies, and the IFRC RFL personnel must comply with when processing data within the framework of RFL activities, in order to:

- comply with applicable data protection standards and legislation;
- allow the seamless flow of personal data needed for RFL activities;
- protect the fundamental rights and freedoms of the enquirer(s), sought person(s) and other individuals such as witnesses or other family members, related to RFL activities according to International Humanitarian Law (IHL), International Human Rights Law and other international standards, in particular the right to privacy and to the protection of personal data.

The Code of Conduct is merely for internal use as it applies to ICRC, National Societies, and the IFRC RFL personnel, or data controllers' RFL activities and RFL-related activities. In the framework of the Code of Conduct data controller is any component of the Movement, which, alone or jointly with others, determines the purposes and means of the processing of personal data.[344]

6.4.5 Resolution on Restoring Family Links while respecting privacy, including as it relates to personal data protection

Resolution 33IC/19/R4 notes the concern regarding families separated and people going missing because of armed conflicts, disasters and other emergencies and recalls the longstanding cooperation between States and the International Red Cross and Red Crescent Movement to restore family links. The Resolution highlights its concern that humanitarian organizations may come under pressure to provide personal data collected for humanitarian purposes to authorities wishing to use such data for other purposes.[345]

[343] https://www.icrc.org/en/document/rfl-code-conduct
[344] Code of Conduct, p. 10.
[345] Resolution 33IC/19/R4, p. 2.

The Resolution recalls that the Movement processes personal data under the framework set out in the Restoring Family Links Code of Conduct on Data Protection and recognized the difficulty, and often impossibility, of acquiring consent in cases of missing or separated families, and the necessity that components of the Movement continue to rely upon alternative valid bases for processing of personal data. The Conference welcomed the Movement's efforts to proactively address and provide adequate safeguards against the risks associated with personal data processing and encouraged the Movement to continue to enhance the effectiveness of data processing practices.[346]

6.4.6 Other

The role of the Data Protection Office is to ensure that ICRC delegations comply with the ICRC Rules in the course of ICRC activities and, to a lesser extent, assist National Societies to comply with data protection standards when there is a need. Also, National Red Cross/Red Crescent offices are sometimes provided with assistance related to personal data. Currently the ICRC Data Protection Office is not engaged with states for the purposes of capacity-building in the area of data protection and privacy.[347]

The model pledge on RFL and Domestic frameworks related to privacy, as it relates to personal data protection, was prepared by the RFL Leadership Platform and the RFL Strategy Implementation Group for components of the Movement and States. It relates to the 33rd International Conference of Red Cross and Red Crescent and is intended for the period 2019-2023.[348]

The objective of the model pledge is to facilitate the delivery of RFL services by the components of the Movement and to ensure the adoption of legislative measures that recognize the important grounds of public interest and in many cases, the vital interests of beneficiaries of RFL services as valid bases for the exclusively humanitarian purpose of such processing. Signatories of pledges commit to:

- working towards the adoption of all necessary domestic legislative, administrative and practical measures in order to implement stringent standards and regulatory frameworks on privacy, including as it relates to personal data protection,
- ensuring that the adoption of legislation and other such measures recognize the public interest and the vital interests of individuals as valid bases for data processing for humanitarian purposes and therefore facilitate the flow of data within the Movement and the effective performance of RFL services in accordance with the Fundamental Principles of neutrality, impartiality and independence.

6.5 The International Criminal Police Organization (INTERPOL)

6.5.1 Rules on the Control of Information and Access to INTERPOL's Files

The Rules relating to the Control of Information and Access to INTERPOL's Files were adopted in the 73rd General Assembly session in 2004 and amended in 2009. The aim of the present Rules is to organize the independent control of INTERPOL's files. A Commission is established for the Control of INTERPOL's Files

[346] Resolution 33IC/19/R4, p. 3-4.
[347] Sarah Safaa DWIDAR, 25 January 2021.
[348] The Model Pledge can be found as Appendix 1.

and governs the composition, role and functions of that Commission. The Rules also set out the general conditions under which a person may gain access to the Organization's files.[349]

Article 9 of the Rules is related to access conditions and procedures and states that any person who so wishes may, freely and free of charge, exercise the right of access to personal information concerning her or him which has been recorded in INTERPOL's files. It further states that requests for access to personal information shall only be admissible if they emanate from persons who may actually be the subject of such information or from the duly authorized or legal representatives of such persons.

6.5.2 INTERPOL's Rules on the Processing of Data

INTERPOL's Rules on the Processing of Data were adopted in 2011 in the 80th General Assembly session, by the Resolution AG-2011-RES-07 and are continually updated to keep pace with technological developments and evolving international data protection standards. The Rules deal with all data processing activities in the INTERPOL Information System, ensuring the efficiency and quality of international cooperation between criminal police authorities through INTERPOL channels, as well as due respect for the basic rights of the individuals who are subjects of this cooperation, in conformity with Article 2 of the Organization's Constitution and the UDHR to which the said Article refers.

The Rules apply in relation to data and personal data and include a definition for 'particularly sensitive data.' The latter comprises any personal data revealing racial or ethnic origin, political opinions, religious or philosophical convictions, trade-union membership, or concerning health or sexuality.[350]

Articles 10 to 18 of the Rules comprise the principles concerning information processing:

Purposes of international police cooperation	The processing of data in the INTERPOL Information System may only be carried out for a given, explicit purpose which is in conformity with the Organization's aims and activities.
Lawfulness	Data processing in the INTERPOL Information System should be authorized with due regard for the law applicable to the National Central Bureau, national entity or international entity and should respect the basic rights of the persons who are the subject of the cooperation, in accordance with Article 2 of the Organization's Constitution and the UDHR.
Quality	Data processed in the INTERPOL Information System must be accurate, relevant, not excessive in relation to their purpose and up to date, to allow them to be used by National Central Bureaus, national entities and international entities.
Transparency	The processing of data in the INTERPOL Information System should guarantee at all times that the processing rights of National Central Bureaus, national entities and international entities are respected in accordance with the present Rules. The General Secretariat shall be responsible for ensuring

[349] Rules on the Control of Information and Access to INTERPOL's Files, Article 1.
[350] Article 1 of the Rules on the Processing of Data, 2009.

	the transparency of data-processing operations and of the functioning of the Organization's databases. The General Secretariat shall keep an up-to-date list of the maximum data retention periods as defined by the Executive Committee in accordance with these Rules and shall make this list publicly available.
Confidentiality	The confidentiality of data processed in the INTERPOL Information System should be determined according to the risks linked to their disclosure for those who are the subject of cooperation, the sources and the Organization. Data should only be accessible to persons authorized to know such information. All necessary and appropriate measures shall be taken to increase the confidentiality level attached to data to protect against risks that their disclosure may have for those who are the subject of cooperation, the sources of data and the Organization.
Security	All appropriate measures shall be taken to protect the security of data processed in the INTERPOL Information System.
External processing for police purposes	The data initially processed in the INTERPOL Information System may be processed outside the system if this processing is necessary and carried out for police purposes. Any external processing must follow the above-mentioned data-processing principles.
Effective implementation	The Rules must be effectively implemented.
Rights of access, correction and deletion of data	Any person or entity shall be entitled to submit directly to the Commission for the Control of INTERPOL's Files a request for access to, or correction and/or deletion of data processed in the INTERPOL Information System concerning that person or entity. These rights of access to, or correction and deletion of data shall be guaranteed by the Commission for the Control of INTERPOL's Files and be governed by separate rules. Unless otherwise specified in those rules, requests for access to, or correction and/or deletion of data may not be processed in the INTERPOL Information System.

Article 112 of the Rules with regard to Confidentiality levels, comprises three confidentiality levels to be established reflecting the increasing risks that may arise from unauthorized disclosure of data: (a) "INTERPOL FOR OFFICIAL USE ONLY" (b) "INTERPOL RESTRICTED" (c) "INTERPOL CONFIDENTIAL". Article 118 of the Rules concerns security incidents and requires the source of that data and different entities to be informed in the event of intrusion or serious attempted intrusion, or violation or attempted violation of the integrity or confidentiality of data.

7 Conclusions

Without much in the way of accompanying analysis, this document has attempted to merely chart UN policy and guidance in the area of data protection and privacy, both the normative framework (as approved by the relevant Member State organs), the further advisory guidance of the various UN Special Rapporteurs, and the in-house policies of UN Secretariat Departments, and various UN agencies, funds and programmes. To showcase the different approaches of other global organisations, we have also included selected policies and guidance as approved and practiced by organisations such as the African Union, the European Union, INTERPOL, and the World Bank Group.

Some of the instruments are intended as instructions for states or other organizations to include the principles in their laws, rules or guidance. Others are intended for the organizations to regulate how the organization is to process personal data. Another important function of the guidance is to show that the organizations have data protection and privacy requirements to follow so that data subjects, clients and partners do want to cooperate with them and are confident enough to transfer personal data to them. Following the entry into force of the EU's GDPR, many organizations and countries have started to update their privacy and data protection policies in order to be in line with the requirements of the GDPR (and its heavy fine-setting environment). However, most of the concepts of the GDPR are not new but have been established already in earlier data protection instruments.

The following table presents eight data protection and privacy protection instruments selected from Chapters 4, 5 and 6 of the research in comparison with common data protection principles that can be found in the GDPR and in other instruments reviewed in this research (and which could be considered as particularly important for legal identity systems). The number after each principle tells how many of the instruments includes the said principle.

It is not straightforward, however, to make conclusions about provisions of legal relevance. It can be seen from the table, for example, that the GDPR does not have a provision regarding interoperability. Recital 68 of the GDPR, however, mentions interoperability by stating that data controllers should be encouraged to develop interoperable formats that enable data portability while the UNECA Principles of Digital ID provide that digital identity systems should be interoperable between Member States, allowing the unique digital identities authenticated by their own system to recognized by other countries. Therefore, deeper research as well as interpretation would be needed to have exact comparison results. For the purpose of this research, the comparison is sufficient.

There are a number of points, however, that run through all of the policy documents drawn upon in this research. Databases containing data on millions of people, for example, are highly sensitive and present an attractive target for attacks by criminal actors. Strong legal, institutional and technical safeguards are therefore required to protect the legal identity systems and personal data in them against unauthorized access and limit their use to the extent necessary for the delivery of public services and prevent overly intrusive use. Data breaches can facilitate identity theft, and in particular, when connected with biometric information, the consequences for the data subjects can be dreadful.[351]

[351] UNCT Operational Guidelines, p. 25.

Data protection Guidance	Regulation (EU) 2016/679	Policy on the Protection of Personal Data of Persons of concern to UNHCR (2018)	Responsible Data for Children - Principles (2019)	ECA Principles of Digital ID	UN Global Pulse Principles on Data Protection and Privacy (2020)	ICRC Handbook on data protection in humanitarian action (2020)	Joint Statement on Data Protection and Privacy in the COVID-19 Response (2020)	UNDP Privacy Principles (2021)
Lawfulness and fairness (7)	GDPR Article 5.1 (a)	Legitimate and fair processing (3)	Participatory and People centric	-	Fair and Legitimate Processing	The principle of the fairness and lawfulness of processing (2.5.1)	Organisations should at minimum be lawful, limited in scope and time, and necessary and proportionate to specified and legitimate purposes in response to the COVID-19 pandemic.	Safeguard personal data (1)
Transparency (7)	GDPR Article 5.1 (a)	Legitimate and fair processing (3)	Professionally accountable	-	Transparency	Specific processing situations and technologies (Part 2)	Be transparent in order to build trust in the deployment of current and future efforts alike.	Safeguard personal data (1)
Purpose limitation (7)	GDPR Article 5.1 (b)	Purpose specification (4.1)	Purpose driven	-	Purpose Specification	The Purpose limitation principle (2.5.2)	Be lawful, limited in scope and time, and necessary and proportionate to specified and legitimate purposes in response to the COVID-19 pandemic.	Safeguard personal data (1) and Make data open by default (4)
Data minimization (5)	GDPR Article 5.1 (c)	-	Proportional	-	Proportionality and Necessity	The principle of Data Minimisation (2.5.4)	-	Safeguard personal data (1)
Proportionality (7)	GDPR Article 6 (lawfulness)	Necessity and Proportionality (4.2)	Proportional	-	Proportionality and Necessity	The Principle of Proporitionality (2.5.3)	Be lawful, limited in scope and time, and necessary and proportionate to specified and legitimate purposes in response to the COVID-19 pandemic.	Safeguard personal data (1)
Accuracy (6)	GDPR Article 5.1 (d)	Accuracy (4.3)	Prevention of harms across the data life cycle	-	Accuracy	The principle of Data Quality (2.5.5)	-	Safeguard personal data (1)
Right to rectification (3)	GDPR Article 16	Respect for the Data Subject's Rights (2.6)	-	-	-	Rights of Data Subject (12.5)	-	-
Right to erasure (3)	GDPR Article 17	Retention, disposal and return of data (4.4)	-	-	-	Rights of Data Subject (12.5)	-	-
Storage limitation (7)	GDPR Article 5.1 (e)	Retention, disposal and return of data (4.4)	Proportional	-	Retention	The principle of Data Minimisation (2.5.4)	Ensure appropriate confidentiality, security, time-bound retention and proper destruction or deletion of data in accordance with the aforementioned purposes.	Safeguard personal data (1)
Integrity and confidentiality (7)	GDPR Article 5.1 (f)	Confidentiality (4.5)	Prevention of harms across the data life cycle	-	Confidentiality	Data Security and Processing Security (2.8)	Ensure appropriate confidentiality, security, time-bound retention and proper destruction or deletion of data in accordance with the aforementioned purposes.	Confidentiality (6)
Accountability (7)	GDPR Article 5.1	Accountability and Supervision (11)	Professionnaly accountable	Accountability	Accountability	The principle of Accountability (2.9)	-	Safeguard personal data (1)
Security (7)	GDPR 5.1 (f)	Data Security (6)	-	Security and Safeguards	Security	Data Security and Processing Security (2.8)	Ensure appropriate confidentiality, security, time-bound retention and proper destruction or deletion of data in accordance with the aforementioned purposes.	Manage data responsibly (3)
Risks, harms and benefits assessment (4)	-	Data Protection Impact Assessments (4.5)	Protective of children's rights and Prevention of harms across the data life cycle	-	Risks, Harms, and Benefits Assessment	Legal bases for personal data processing (6.2.2)	-	-
Due diligence for third party collaborators (2)	-	-	-	-	Technology Collaborators and Data Transfers	Cash transfer programming (Chapter 9)	-	-
No re-identification (2)	-	-	-	-	No Re-identification	Cash transfer programming (Chapter 9)	-	-
Special categories of personal data (4)	GDPR Article 9	Data Security (6.1.2)	-	-	Data Sensitivity	Health Purposes (2.6.1)	-	-
Data protection by design (4)	GDPR Article 25	Privacy by Design and Default (6.4)	-	-	-	Data protection by Design (11.9) and others	-	Safeguard personal data (1)
Data Breach Notification (4)	GDPR Articles 33-34	Notification of a Personal Data Breach (4.4)	-	-	-	Data Security (10.4) and others	-	Manage Data responsibly (3)
Data portability (4)	GDPR Article20	-	-	Interoperability	-	Data Security (10.4)	-	Plan for reusability and interoperability
Interoperability (3)	-	-	-	Interoperability	-	Data Security (10.4)	-	Plan for reusability and interoperability (5)

To conclude, the following principles, subject to regulatory changes, should be considered as minimum safeguards when UN Member States are processing personal data, particularly in the framework of legal identity systems:

DATA PROTECTION AND PRIVACY PRINCIPLES IN THE FRAMEWORK OF LEGAL IDENTITY SYSTEMS	
Lawfulness, fairness and transparency	Each piece of personal data and each processing activity shall have a legitimate objective and be necessary for legal, statistical or identity management purposes.
	In particular, official identity documents shall include only relevant, reasonable and necessary personal information, as required by law for a legitimate purpose.
	Personal data shall be processed in a transparent manner in relation to the data subject.
Purpose limitation	Personal data shall be collected for legal, statistical or identity management purposes and not further processed in a manner that is incompatible with the purpose.
Data minimization	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose of particular component of the legal identity system.
Accuracy	Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
	Updating personal data following any occurrence of events vital to individuals, including change of name or gender, or death, shall be carried out without delay and in accordance with national legislation.
Rights of Data Subject	The data subject shall obtain access to all data concerning him or her in a transparent manner.
	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning her or him.
	The data subject shall have the right to obtain from the controller the erasure his or her personal, and the controller shall erase personal data, without undue delay in case the personal data are no longer necessary in relation to the legal identity system.
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of the legal identity system.

Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
Data Breach Notification	In case of a personal data breach the controller shall communicate the data breach appropriately, without undue delay, in its organization. The data subjects shall be informed of the data breach in case it is of significant scale or may cause significant harm to the data subjects.
Accountability and remedies	Controllers of the legal identity system shall be responsible for and be able to demonstrate compliance with all requirements of Principles such as these.
	Administrative and judicial measures should be taken to remedy excessive and other unlawful data processing, as well as breach of the rights and interests of the data subject.
	Any data subject who has suffered material or non-material damage as a result of an infringement of Principles such as these should have right to compensation from the controller/processor for damage suffered.
Risks, harms and benefits assessment	A risks, harms and benefits assessment that accounts for data protection and data privacy as well as ethics should be conducted regularly once a year and prior to the introduction of new processing activities or new personal data categories in the legal identity system, or substantial changes of the above.
Due diligence for third party collaborators	Due diligence should be conducted to evaluate the practices of any potential third-party collaborators in the framework of legal identity systems.
Data protection by design and by default	Privacy and data protection should be primary concerns at the initial design stage and throughout the complete development process of legal identity systems and any substantial change in it.
	Appropriate technical and organisational measures should be implemented for ensuring that, by default, only personal data necessary for the purpose of the legal identity system are processed.
Data Portability and interoperability	The data subject should have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.
	Digital identity systems should, as much as is feasible, be interoperable between UN Member States, allowing unique digital identities authenticated by their own system to be recognized by other countries.

References

Title	Available at
Implementation of the United Nations Legal Identity Agenda: United Nations Country Team Operational Guidelines	Home — UN Legal Identity Agenda
Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management. 2019	https://unstats.un.org/unsd/demographic-social/Standards-and-Methods/files/Handbooks/crvs/CRVS_GOLF_Final_Draft-E.pdf
'How the Right to Privacy Became a Human Right' by Oliver Diggelmann and Maria Nicole Cleis in Human Rights Law Review, 2014 of 7 July 2014	https://www.corteidh.or.cr/tablas/r33348.pdf.
The Long and Influential Life of the Universal Declaration of Human Rights in THE UNIVERSAL DECLARATION OF HUMAN RIGHTS IN THE 21ST CENTURY. Ed. Gordon Brown	https://books.openedition.org/obp/3058?lang=en#text
United Nations Country Team Operational Guidelines	https://unstats.un.org/legal-identity-agenda/documents/UNCT-Guidelines.pdf
Security Council Guiding Principles on Foreign Terrorist Fighters	https://www.un.org/sc/ctc/wp-content/uploads/2019/09/Security-Council-Guiding-Principles-on-Foreign-Terrorist-Fighters.pdf
United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter Terrorism (in association with the Biometrics Institute)	https://www.un.org/sc/ctc/wp-content/uploads/2018/08/Compendium-Final-Draft-June-18.pdf
The European Data Protection Supervisor Strategy 2020-2024	https://edps.europa.eu/edps-strategy-2020-2024/
The Charter of the United Nations	https://www.un.org/en/sections/un-charter/chapter-xvi/index.html
UN Department of Peace Operations	https://peacekeeping.un.org/sites/default/files/dppa-dpo-org-chart-2019.pdf
UN Department of Political and Peacebuilding Affairs, 'what we do'	https://dppa.un.org/en/what-we-do
UN Department of Peace Operations, 'About us'	https://peacekeeping.un.org/en/department-of-peace-operations

Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping	https://peacekeeping.un.org/sites/default/files/performance-peacekeeping_expert-panel-on-technology-and-innovation_report_2015.pdf
UN Roadmap for Digital Cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation Report of the Secretary-General	https://undocs.org/A/74/821
UN Global Data Access Framework	https://www.unglobalpulse.org/policy/global-data-access-framework/
ICAO Trip Guide on Border Control Management	https://www.icao.int/security/fal/trip/pages/publications.aspx
ICRC Rules on Personal Data Protection	https://shop.icrc.org/icrc-rules-on-personal-data-protection-pdf-en
ICRC Policy on the Processing of Biometric Data, August 2019	https://www.icrc.org/en/document/icrc-biometrics-policy
ICRC Restoring Family Links Code of Conduct on Data Protection	https://www.icrc.org/en/document/rfl-code-conduct
ICRC Restoring Family Links while respecting privacy, including as it relates to personal data protection. Resolution 33IC/19/R4 (December 2019)	https://www.cervenykriz.eu/files/files/cz/781/R4.pdf
'Georgia pledges to effectively implement/enforce personal data protection legislation by supporting the data protection authority – State Inspector's Service of Georgia in performing its function'	Georgia pledges to effectively implement/enforce personal data protection legislation by supporting the data protection authority – State Inspector's Service of Georgia in performing its function – Statutory Meetings (rcrcconference.org)
'Mapping the current legal and administrative framework and practices related to privacy about personal data protection in Ethiopia'	Mapping the current legal and administrative framework and practices related to privacy about personal data protection in Ethiopia – Statutory Meetings (rcrcconference.org)
ILO Protection of Workers' Personal Data	https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf
ILO Policy Brief, 'Minimum requirements for ensuring privacy and data protection in social protection systems.' Social Protection for All Issue Brief, June 2018	https://www.social-protection.org/gimi/RessourcePDF.action?id=55904
IOM data protection website	https://www.iom.int/data-protection
IOM Data Protection Manual, 2010	https://publications.iom.int/books/iom-data-protection-manual

Workshop: Data Protection within International Organizations	https://edps.europa.eu/data-protection/our-work/publications/events/workshop-data-protection-within-international_en
UN Privacy Policy Group (UN PPG)	https://www.unglobalpulse.org/policy/un-privacy-policy-group/
'IOM Republic of Korea Hosts Workshop on Data Collection and Needs Assessment for Humanitarian Project Design,' 29 June 2020	https://reliefweb.int/report/republic-korea/iom-republic-korea-hosts-workshop-data-collection-and-needs-assessment
United Nation's Privacy Notice	https://www.un.org/en/sections/about-website/privacy-notice/index.html
Terms and Conditions of Use of United Nations Web Sites	https://www.un.org/en/sections/about-website/terms-use/index.html
UN Fraud Alert	https://www.un.org/en/sections/about-website/fraud-alert/index.html
UN Principles Governing International Statistical Activities	https://unstats.un.org/unsd/methods/statorg/Principles_stat_activities/principles_stat_activities.asp
UN Good Practices on National Official Statistics	https://unstats.un.org/unsd/dnss/gp/gpintro.aspx
Resolution adopted by the Economic and Social Council on 24 July 2013, (E/2013/24) 2013/21. Fundamental Principles of Official Statistics	https://unstats.un.org/unsd/dnss/gp/FP-Rev2013-E.pdf
Resource Materials on Data Privacy Laws in Asia and the Pacific - Webinar on Data Privacy Laws in ASEAN, (UNESCAP and APCICT)	https://www.unapcict.org/sites/default/files/2021-01/Resource%20Materials%20on%20Data%20Privacy%20Laws%20in%20Asia%20and%20the%20Pacific.pdf
Myanmar Webinar on Data Protection and Privacy. 25-28 January 2021	https://www.unescap.org/events/2021/myanmar-webinar-data-protection-and-privacy
African Union Convention on Cyber Security and Personal Data Protection	https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
Digital ID, Digital Trade, and Digital Economy in Africa	https://www.uneca.org/dite-africa
Concept note on the ECA on Digital Identity, Trade and Economy Initiative and Center of Excellence	https://www.uneca.org/sites/default/files/uploaded-documents/DITE-Africa/concept-note.pdf
Africa Data Leadership Initiative	https://futurestate.org/adli/
https://www.unglobalpulseorg/policy/ungp-principles-on-data-privacy-and-prote%20a,carrying%20out%20their%20mandated%20activities.&text=(iii)%20ensure%20res	

pect%20for%20the,particular%20the%20right%20to%20privacy	
UN Global Pulse Principles on Data Protection and Privacy	https://www.unglobalpulse.org/policy/ungp-principles-on-data-privacy-and-protection/
Expert Group on Governance of Data and AI	https://www.unglobalpulse.org/policy/expert-group-on-governance-of-data-and-ai/
Global Data Access Framework	https://www.unglobalpulse.org/policy/global-data-access-framework/
UNFPA Privacy Policy	https://www.unfpa.org/unfpa-privacy-policy
Alexander Beck, Senior Data Protection Officer, on the particular role of data protection for UNHCR (May 23rd, 2018)	https://www.unhcr.org/blogs/data-protection-part-parcel-refugee-protection/
Data protection is part and parcel of refugee protection (23 May 2018)	https://www.unhcr.org/blogs/data-protection-part-parcel-refugee-protection/
Policy on the Protection of Personal Data of Persons of concern to UNHCR	https://www.unhcr.org/privacy-policy.html
UNHCR Guidance on Registration and Identity Management	https://www.unhcr.org/registration-guidance/
UNHCR Privacy Policy	https://www.unhcr.org/privacy-policy.html
UNHCR Data Transformation Strategy	https://www.unhcr.org/5dc2e4734.pdf
UN Joint Staff Pension Fund Privacy Policy	United Nations Joint Staff Pension Fund » Privacy Notice (unjspf.org)
UNJSPF 'Your Pension Data Security'	United Nations Joint Staff Pension Fund » Your Pension Data Security (unjspf.org)
'About the UN Counter-Terrorism Committee'	https://www.un.org/sc/ctc/about-us/
UN Security Council Guiding Principles on Foreign Terrorist Fighters	https://www.un.org/sc/ctc/wp-content/uploads/2019/09/Security-Council-Guiding-Principles-on-Foreign-Terrorist-Fighters.pdf
Resolution 2396 (2017)	https://undocs.org/en/S/RES/2396(2017)
United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter Terrorism	https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf
Counter-Terrorism Travel Programme Summary, 'Building the Capacity of Member States to Prevent, Detect and Investigate Terrorist Offenses and Related Travel by Using	https://www.un.org/cttravel/content/summary

Advance Passenger Information (API) and Passenger Name Record (PNR) Data'	
IOM Community Response App	https://www.iom.int/community-response-app
'IATA and UNOCT to Cooperate on Countering Terrorist Travel'	https://www.iata.org/en/pressroom/pr/2020-09-24-01/
'CARICOM IMPACS and the United Nations Office of Counter-Terrorism (UNOCT) collaborate to detect and counter terrorists and serious criminals' travel using passenger data'	https://www.un.org/cttravel/news/caricom-impacs-and-united-nations-office-counter-terrorism-unoct-collaborate-detect-and-counter
UNICEF Policy on Personal Data Protection Document Number: POLICY/DFAM/2020/001 Effective Date: 15 July 2020	https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf.pdf,
UNICEF Procedure for Ethical Standards in Research, Evaluation, Data Collection and Analysis	https://www.unicef.org/media/54796/file
Responsible Data for Children – Synthesis Report – RD4C.org	https://rd4c.org/files/rd4c-report-final.pdf
UNICEF guidance on the use of biometrics in children-focused services	https://data.unicef.org/resources/biometrics/
DISCUSSION PAPER SERIES: Children's Rights and Business in a Digital World	https://sites.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf
UN Women, Information Security.	https://www.unwomen.org/en/about-the-website/information-security
UN Women, Privacy Notice.	https://www.unwomen.org/en/about-the-website/privacy-notice
World Health Organization Data Principles, 10 August 2020	https://www.who.int/docs/default-source/world-health-data-platform/who-data-principles-10aug-(3).pdf?sfvrsn=3d89acf0_6
WHO Privacy Policy	https://www.who.int/about/who-we-are/privacy-policy
Policy on use and sharing of data collected in Member States by the World Health Organization (WHO) outside the context of public health emergencies (Provisional), August 2017	https://www.who.int/docs/default-source/publishing-policies/who-data-sharing-policy-collected-by-member-states-outside-of-public-health-emergencies61d03608e6134ba786ad94403e947013.pdf?sfvrsn=bb52b31d_31
Policy statement on data sharing by WHO in the context of public health emergencies (as of 13 April 2016).	https://www.who.int/wer/2016/wer9118.pdf?ua=1
World Food Programme, Overview	https://www.wfp.org/overview

WFP Guide to Personal Data Protection and Privacy, June 2016	https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/
Submissions from entities in the United Nations system, international organizations and other stakeholders on their efforts in 2019 to implement the outcomes of the WSIS Submission by WFP, March 2020	https://unctad.org/system/files/non-official-document/a75d62_bn_WFP.pdf
The World Bank Group Personal Data Privacy Policy	http://documents1.worldbank.org/curated/en/466121527794054484/pdf/Privacy-Board-Paper-050318-vF-05042018.pdf
UN Secretary-General's High-Level Panel on Digital Cooperation	HLP on Digital Cooperation Press Release - Published (un.org)
Report of the UN Secretary-General's Roadmap for Digital Cooperation Report	https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf
Data Strategy of the UN Secretary General for Action by Everyone, Everywhere	https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy-one-pager.pdf
The UN Secretary-General's Data Strategy adopted by the UN System Chief Executives Board for Coordination and the implications for FAO	http://www.fao.org/3/nd228en/nd228en.pdf
Guidance Note on Big Data for Achievement of the 2030 Agenda	https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf
Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020-22	https://www.un.org/en/sections/issues-depth/big-data-sustainable-development/
Joint Statement on Data Protection and Privacy in the COVID-19 Response	https://www.un.org/sites/un2.un.org/files/joint_statement_on_data_protection_and_privacy_in_covid-19_response.pdf
ICC Helps with UN Principles on Personal Data Protection and Privacy	https://www.unicc.org/news/2019/02/11/icc-helps-with-un-principles-on-personal-data-protection-and-privacy/
UN/DESA Policy Brief #89: Strengthening Data Governance for Effective Use of Open Data and Big Data Analytics for Combating COVID-19	https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-89-strengthening-data-governance-for-effective-use-of-open-data-and-big-data-analytics-for-combating-covid-19/
Air Law and Aviation Industry of the future	https://www.icao.int/Meetings/SingaporeSeminar2019/Documents/2_3_Bader_Almubarak_-_Personal_Data_Protection___Climate_Change.pdf

About ICAO	https://www.icao.int/about-icao/Pages/default.aspx
Guidelines on Advance Passenger Information (API) WCO/IATA/ICAO, 2014	https://www.icao.int/Security/FAL/SiteAssets/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards/API-Guidelines-Main-Text_2014.pdf
Standards and Principles on the collection, use, processing and protection of passenger name record (PNR) data	https://www.icao.int/Meetings/a40/Documents/WP/wp_530_en.pdf#search=personal%20data
Implementation of API: UN Security Council Resolution 2178 and 2309	https://www.icao.int/ESAF/AFI-Aviation-Week-2017/Documents/Second%20AFI%20Security%20Symposium/Implementation%20of%20UN%20Security%20Council%20resolutions%202178%20and%202309.pdf#search=api