DATA PRIVACY, ETHICS AND PROTECTION

GUIDANCE NOTE ON BIG DATA FOR ACHIEVEMENT OF THE 2030 AGENDA

UNITED NATIONS DEVELOPMENT GROUP

This document has been approved through the United Nations Development Group (UNDG) and applies to all member entities within the UNDG and its working mechanisms. The approval of this document is based on consensus among UNDG members and the provisions contained herein 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.

TABLE OF CONTENTS

PURPOSE OF THIS GUIDANCE NOTE

This document sets out general guidance on data privacy, data protection and data ethics for the United Nations Development Group (UNDG) concerning the use of big data, collected in real time by private sector entities as part of their business offerings[1], and shared with UNDG members for the purposes of strengthening operational implementation of their programmes to support the achievement of the 2030 Agenda[2]. The Guidance Note is designed to:

- Establish common principles across UNDG to support the operational use of big data for achievement of the Sustainable Development Goals (SDGs);
- Serve as a risk-management tool taking into account fundamental human rights; and
- Set principles for obtaining, retention, use and quality control for data from the private sector.

The **data revolution** was recognized as an enabler of the Sustainable Development Goals, not only to monitor progress but also to inclusively engage stakeholders at all levels to advance evidence-based policies and programmes and to reach the most vulnerable.[3] The 2030 Agenda asserts that "Quality, accessible, timely and reliable disaggregates data will be needed to help with the measurement of progress (SGDs) and to ensure that no one is left behind. Such data is key to decision making."[4]

At the same time, there are legitimate concerns regarding risks associated with handling and processing of big data, particularly in light of the current fragmented regulatory landscape and in the absence of a common set of principles on data privacy, ethics and protection. These concerns continue to complicate efforts to develop standardized and scalable approaches to risk management and data access. A coordinated approach is required to ensure the emergence of frameworks for safe and responsible use of big data for the achievement of the 2030 Agenda.

The guidance described in this document acknowledges and is based on the UN Guidelines for the Regulation of Computerized Personal Data Files, adopted by the UN General Assembly resolution 45/95, and takes into account both existing international instruments and relevant regulations, rules and policies of UNDG member organizations concerning data privacy and data protection. This Guidance Note is based on standards that have withstood the test of time, reflecting the strength of their core values.

This Guidance Note is designed to support members and partners of the UNDG in establishing efficient and coherent data collaborations.

1 This Guidance Note focuses on the use of big data collected by non-UN parties. Many of the guiding principles, however, may be applied in cases where UNDG members collect big data for the purposes of implementing their mandates, for example in the form of photographs or videos collected by unmanned aerial vehicles (UAVs).

2 This Guidance Note supports implementation of the Quadrennial Comprehensive Policy Review of the operational activities for development of the UN system (A/C.2/71/L.37), particularly in its call for the UN funds, programmes and specialized agencies to strengthen their support to "collect, analyse and increase significantly the availability of high-quality, timely and reliable disaggregated data....and in so doing utilizing national capacities to the fullest extent possible in the context of United Nations operational activities for development."

3 Examples of how big data could be used to support the Sustainable Development Goals can be viewed in Addendum A.

4 For more detail, see Transforming our World: The 2030 Agenda for Sustainable Development (A/RES/70/1, p. 11), available at https://sustainabledevelopment.un.org/post2015/transformingourworld.

5 The right to privacy is enshrined by the Universal Declaration of Human Rights, Article 12 (UN General Assembly resolution 217 A(III), Paris, France, 10 December 1948.; the International Covenant on Civil and Political Rights, Article 17 (General Assembly resolution 2200 A(XXI), New York, 19 December 1966, UN Treaty Series, vol. 999, No. 14668, p. 171 and vol. 1057, p. 4019); the Convention on the Rights of the Child (art. 16), the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14); European Convention on Human Rights (art. 8); the American Convention on Human Rights (art. 11).

Reaffirming that the right to privacy is a fundamental human right and recognizing the social value of data, including the value of disaggregated SDG indicators with regard to the implementation of the 2030 Agenda, this document aims to provide a harmonized general framework for accountable, adequately transparent, and responsible data handling practices across the UNDG and with partners.

This Guidance Note is not a legal document. It provides only a minimum basis for self-regulation, and therefore may be expanded and elaborated on by the implementing organizations.

Acknowledging the potential risks and harms as well as the benefits that can result from big data use, this document goes beyond individual privacy and considers potential effects on group(s) of individuals. Additionally, this guidance takes into consideration standards of moral and ethical conduct, and recognizes the importance of context when big data is being used.

It is recommended that this Guidance Note be implemented through more detailed operational guidelines that account for the implementation of UNDG member organizations' mandates as well as their existing regulations, rules and policies concerning data privacy, data protection, data ethics and data security. It is recommended that designated legal, ethics, privacy and security experts be consulted, when necessary, regarding the implementation of, and compliance with, this Note. Implementing organizations are encouraged to establish a monitoring mechanism for compliance and implementation of this Note.

Given continuous advances in technology and data, the international landscape concerning data privacy and data protection (including through the relevant work of the UN) may also change. Accordingly, this note is a living document and may also evolve over time.

UNDG is grateful to UN Global Pulse for developing this Guidance Note and acknowledges the invaluable contributions of the Global Pulse Privacy Advisory Group as well as other private and public expert stakeholders. Any questions, comments or recommendations regarding this Guidance Note should be directed to kit.doco@undg.org.

6 Sustainable Development Goal 17 aims to "Strengthen the means of implementation and revitalize the global partnership for sustainable development". Target 17.18 notes the need for data disaggregation by income, gender, age, race, ethnicity, migratory status, disability, geographic location and other characteristics relevant in national contexts (A/70/L.1.).

7 For more information, see the "Report of the Special Rapporteur on the right to privacy", Joseph A. Cannataci, Annex II. A more in-depth look at Open Data and Big Data (A/HRC/31/64, p. 24).

PRINCIPLES

1. LAWFUL, LEGITIMATE AND FAIR USE

Data access, analysis or other use must be consistent with the United Nations Charter and in furtherance of the Sustainable Development Goals.

Whether directly or through a contract with a third party data provider, 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.

Data should always be accessed, analysed or otherwise used taking into account the legitimate interests of those individuals whose data is being used. Specifically, to ensure that data use is fair, data should not be used in a way that violates human rights, or in any other ways that are likely to cause unjustified or adverse effects on any individual(s) or group(s) of individuals. It is recommended that legitimacy and fairness of data use is always assessed taking into account risks, harms and benefits as discussed in Section 6.

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): (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.

2. PURPOSE SPECIFICATION, USE LIMITATION AND PURPOSE COMPATIBILITY

Any data use must be compatible or otherwise relevant, and not excessive in relation to the purposes for which it was obtained. The purpose of data use cannot be changed unless there is a legitimate basis, as noted in Section 1. The purpose should be legitimate and as narrowly and precisely defined as practically possible. Requests or proposals for data access should be tailored to a specific purpose.

There must be a legitimate and fair basis for an incompatible deviation from the purpose for which the data was obtained. However, mere difference in purpose does not make a new purpose incompatible. In determining compatibility, for example the following criteria could be considered: how deviation from the original purpose may affect an individual(s) or group(s) of individuals; or the type of data used (e.g. public, sensitive or non-sensitive); or measure taken to safeguard the identity of individuals whose data is used (e.g. pseudonymization, masking, encryption).

The purpose of data access (or collection where applicable) should be articulated no later than the time of data access (or collection where applicable).

3. 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. Appropriate risk mitigation measures should be implemented. Individual(s) or group(s) of individuals should not be exposed to harm, or to undignified or discriminatory treatment, as a consequence of data use by UNDG member organizations.

Any risks, harms and benefits assessment should take into consideration the context of data use, including social, geographic, political and religious factors. Such assessments should account for potential physical, emotional or economic harms, as well as any harms that could be caused as a result of infringement of individual(s)' rights.

Any risks, harms and benefits assessment should take into consideration the impact that data use may have on an individual(s) and/or group(s) of individuals, whether legally visible or not and whether known or unknown at the time of data use.

An assessment of harms should consider such key factors as: (i) the likelihood of occurrence of harms, (ii) potential magnitude of harms and (iii) potential severity of harms.

Additionally, the assessment should take into account the digital literacy of both potential users of data and those individuals whose data is being used.

Where possible, the assessment should be completed by a diverse team of experts (e.g. legal, ethics and security experts as well as subject-matter experts) and, where reasonably practical, a representative of the group(s) of individuals who could be potentially affected.

The risk of harm is much higher for sensitive data, and stricter measures for protection should apply if such data is explicit personal data or is reasonably likely to identify an individual(s) or a group(s) of individuals.

Decisions concerning the use of sensitive data should involve consultation with groups concerned (or their representative) where possible to mitigate any associated risks.

Additionally, it is important to take into account risks associated with data breaches and vulnerable data security systems, as noted in Section 3.

Use of data should be based on the principle of proportionality. In particular, any potential risks and harms should not be excessive in relation to the positive impacts (benefits) of data use. Furthermore, assessing the effect of data on individual rights in conjunction with each other is recommended wherever possible, rather than taking rights in opposition to each other.

The risks, harms and benefits assessment can be a tool that helps to assist with determination of whether the use of data is legitimate, appropriate or fair.

4. SENSITIVE DATA AND SENSITIVE CONTEXTS

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.

It is important to consider that context can turn non-sensitive data into sensitive data. The context in which the data is used (e.g. cultural, geographic, religious, the political circumstances, etc.) may influence the effect of the data analysis on an individual(s) or group(s) of individuals, even if the data is not explicitly personal or sensitive.

5. DATA SECURITY

Data security is crucial in ensuring data privacy and data protection. Taking into account available technology and cost of implementation, robust technical and organizational safeguards and procedures (including efficient monitoring of data access and data breach notification procedures) should be implemented to ensure proper data management throughout the data lifecycle and prevent any unauthorized use, disclosure or breach of personal data.

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, in an effort to prevent risks to privacy and harms from arising.

Personal data should be de-identified, where appropriate, using such methods as aggregation, pseudonymization, or masking, for example, to minimize any potential risks to privacy, and taking into account the likely occurrence of any potential harms associated with data use and non-use. Where appropriate, UNDG member organizations should consider working with data that has been de-identified by third party data providers prior to its disclosure to the UNDG member organizations.

Encrypt personal and sensitive data when transferred to or from any network-connected server. No de-identified data should knowingly and purposely be re-identified, unless there is a legitimate, lawful and fair basis as noted in Section 1. To minimize the possibility of re-identification, it is recommended that de-identified data not be analysed or otherwise used by the same individuals who originally de-identified the data.

It is important to ensure that the measures taken to protect privacy and ensure data security do not disproportionately compromise the utility of the data for the intended purpose.

Such measures should be employed in such a way as to maximize the positive impact expected from the data use and to fulfill the purposes for which the data was obtained.

Data access should be limited to authorized personnel, based on the "need-to-know" principle. Personnel should undergo regular and systematic data privacy and data security trainings. Prior to data use, vulnerabilities of the security system (including data storage, way of transfer, etc.) should be assessed.

Data security measures should be assessed in light of the risks, harms and benefits of data use, including as noted in Section 3.

When considering the risks associated with the vulnerability of data security systems, it is important to consider factors such as intentional or unintentional unauthorized data leakage or breach: (i) by authorized personnel, (ii) by known third parties who have requested or may have access, or may be motivated to get access to misuse the data and information, (iii) by unknown third parties (e.g. resulting from publishing data sets or the results of an analysis).

Special attention should be paid when using cloud services, especially with regard to the data security setup and physical locations at which data is stored. Usage of non-cloud storage should be considered for sensitive data. When third-party cloud storage providers are used, potential risks and harms associated with the use of such cloud storage, as detailed in Section 3, should be both taken into account.

6. DATA RETENTION AND DATA MINIMIZATION

Data access, analysis or other use should be kept to the minimum amount necessary to fulfill its purpose, as noted in Section 2.

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.

Any retention of data[8] should have a legitimate and fair basis, including beyond the purposes for which access to the data was originally granted, as specified in Section 1, to ensure that no extra or just-in-case data set is stored. Any data retention should be also considered in light of the potential risks, harms and benefits as discussed in Section 3. The data should be permanently deleted upon conclusion of the time period needed to fulfill its purpose, unless its extended retention is justified as mentioned in this Section above. Any deletion of data should be done in an appropriate manner taking into consideration data sensitivity and available technology.

7. DATA QUALITY

All data-related activities should be designed, carried out, reported and documented with an adequate level of quality and transparency. More specifically, to the extent reasonably possible, data should be validated for accuracy, relevancy, sufficiency, integrity, completeness, usability, validity and coherence, and be kept up to date.

Data quality should be carefully considered in light of the risks that the use of low quality data for decision-making can create for an individual(s) and group(s) of individuals.

Data quality must be assessed for biases to avoid any adverse effects, where practically possible, including giving rise to unlawful and arbitrary discrimination.

9 It is important to emphasize that big data generated by the use of social media, mobile phones, credit cards, etc. is usually owned by either the original author or the digital service provider (e.g. social media platform, mobile phone company or bank).

10 Usually, there will be an opportunity to obtain consent if the organization is the original data collector. However, in situations where data is being obtained from a third party data provider, checking whether a third party data provider has obtained adequate consent (e.g. directly or indirectly through the online terms of use) or has another legitimate basis for collecting and sharing the data is recommended when conducting a due diligence exercise.

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.

8. 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 (including this Guidance Note).

Transparency is a critical element of accountability. Being transparent about data use (e.g. publishing data sets or publishing an organization's data use practices or the use of algorithms) is generally encouraged when the benefits of transparency are higher than the risks and possible harms.

Except in cases where there is a legitimate reason not to do so, at minimum, the existence, nature, anticipated period of retention and purpose of data use as well as the algorithms used for processing data should be publicly disclosed and described in a clear and non-technical language suitable for a general audience.

Open data is an important driver of innovation, transparency and accountability. Therefore, whenever possible, the data should be made open, unless the risks of making the data open outweigh the benefits or there are other legitimate bases not to do so. Disclosure of personal information, even if derived from public data, should be avoided or otherwise carefully assessed for potential risks and harms as described in Section 3.

A risks, harms and benefits assessment (noted in Section 3) should be one of the key accountability mechanisms for every use of data, and should help determine what other governance mechanisms may be needed to monitor compliance. In particular, making data open or being transparent about data uses should be considered a separate stage in the data life cycle, and thus it is recommended that a separate assessment, noted in Section 3, is conducted to address risks, harms and benefits related to that stage. The assessment should help determine the level of openness and transparency.

9. 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. Their actions should be consistent with the United Nations' global mandate as well as UN regulations, rules and policies. Furthermore, third party collaborators' actions should adhere to the Guidance Note, including to have a legitimate and fair basis for sharing data with UNDG member organizations.[9]

It is recommended that a process of due diligence be conducted to evaluate the data practices of any potential third party collaborators.[10]

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.

DEFINITIONS & NOTES

AGGREGATION OF DATA

For the purposes of this document, data aggregation means a process through which individual level data sets are combined to such a format so they cannot be traced back or linked to an individual. Typically, aggregated data is used for analytical or statistical purposes to present a summary or determine average results/numbers regarding age, gender, community preferences, etc.

In addition, the UN Archives and Records Management Section in its "Glossary of Recordkeeping Terms" defines "aggregated records" as referring to "accumulated or collected records that are organized into groupings or series". From the International Organization for Migration (IOM), the IOM Data Protection Manual also defines "aggregate data" as information, usually summary statistics, which may be compiled from personal data, but are grouped in a manner to preclude the identification of individual cases.

ADEQUATE CONSENT

Consent is adequate, when it is freely given, explicit, informed and in writing. Adequate consent should be obtained prior to data collection or when the purpose of data re-use falls outside of the purpose for which consent was originally obtained.

To ensure that consent is informed, it is recommended that as many details about the purpose of data use (e.g. any risks, harms and potential positive and negative impacts) should be included in the notice when the consent is sought. It is important to note that in many instances consent may not be adequately informed. Thus, it is important to consider assessing the proportionality of risks, harms and benefits of data use even if consent has been obtained.

Consent should be obtained before data is collected or otherwise used, and individuals should have an opportunity to withdraw their consent or object to the use of their data. Checking whether a third party data provider has obtained adequate consent (e.g. directly or indirectly through the online terms of use) or has another legitimate basis for sharing the data is recommended.

While there may be an opportunity to obtain consent at the time of data collection, re-use of data often presents difficulties for obtaining consent (e.g. in emergencies where you may no longer be in contact with the individuals concerned). In situations where it is not possible or reasonably practical to obtain informed consent, as a last resort, data experts may

still consider using such data for the best or vital interest of an individual(s) or group(s) of individuals (e.g. to save their life, reunite families, etc.). In such instances, any decision to proceed without consent must be based on an additional detailed assessment of risks, harms and benefits to justify such action and must be found fair, lawful, legitimate and in accordance with the principle of proportionality (e.g. any potential risks and harms should not be excessive in relation to the expected benefits of data use).

BIG DATA

There are many definitions of big data. UN Global Pulse in its report "Big data for development: Challenges and opportunities" takes a traditional approach, defining 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. The characteristics which broadly distinguish big data are sometimes called the '3 V's': more volume, more variety and higher rates of velocity." The report provides examples of such data, including data from sensors used to gather climate information, posts to social media sites, digital pictures and videos posted online, transaction records of online purchases, and from cell phone GPS signals.

There are many types of big data with potential utility for development. This document applies specifically to data collected by the private sector in real time and that may be used for the observation of human behaviour by UNDG, thus affecting the decision-making process with regard to the individual(s) or group(s) of individuals. Usually, such data would be owned by an original author (e.g. a social media user) or a digital service provider (e.g. a social media platform, a mobile phone company, a bank, etc.).

The International Telecommunication Union (ITU), in its recommendation on "Big data – Cloud computing based requirements and capabilities" defines big data as "a paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics".

DE-IDENTIFICATION (ANONYMIZATION) OF DATA

For the purposes of this document, de-identification shall mean a process of using all reasonable means to convert personal data into anonymous data, such as that it cannot be traced back or linked to an individual(s) or group(s) of individuals. There are many different methods that could be used to de-identify data. Examples include data aggregation, masking, pseudonymization and k-anonymity.

De-identified data may be stripped of all personal identifiers such as name, date of birth, exact location, etc.); however, as noted in the UN Global Pulse Data Innovation Risk Assessment Tool guidance, this data, although not directly or explicitly identifying or singling out an individual or group(s) of individuals, can still be **linked** to an individual(s) or group(s) of individuals with the use of adequate technology, skills and intent and thus may require the same level of protection as explicit personal data.

DIGITAL LITERACY

For the purposes of this document, digital literacy means how people understand the data they work with or share, including how much they are aware of the positive and negative impacts of data use and sharing. Digital literacy concerns both actors who are using the data and those whose data is being used.

ENCRYPTION

In the glossary of the UN Archives and Records Management Section, encryption is defined as a "security procedure that translates electronic data in plain text into a cipher code by means of either a code or a cryptographic system in order to render it incomprehensible without the aid of the original code or cryptographic system".

GROUP(S) OF INDIVIDUALS

For the purposes of this document, reference to a group(s) of individuals also includes "legal" invisible (known or unknown) group(s) of individuals, as adapted from the human-rights based approach to data of the Office of the United Nations High Commissioner for Human Rights (OHCHR).

MASKING

For the purposes of this document, masking means a de-identification technique whereby the original personal information collected from social media, such as comments, photos and videos, is altered to such extent that it cannot be traced back or linked to an individual(s) or group(s) of individuals.

PERSONAL DATA

For the purposes of this document, personal data means data, in any form or medium, relating to an identified or identifiable individual who can be identified, directly or indirectly, by means reasonably likely to be used, including where an individual can be identified by linking the data to other information reasonably available. Personal data is defined by many regional and national instruments and can also be referenced as personal information or personally identifiable information.

Personal data can be made private by its owner by restricting access to it or made public by its owner (e.g. shared publicly on social media). While sharing (and oversharing) personal details about oneself and others on social networks has become more common, such publicly available information remains personal and it can pose risks to those individuals represented in the data.

PRIVACY

A report of the Special Rapporteur to the Human Rights Council (A/HRC/23/40) defines privacy as "the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other individuals". While the majority of literature and legislature concentrates on "the right to privacy", in another such report (A/HRC/31/64), it has been noted that there is currently no internationally accepted definition of privacy.

PRIVACY BY DESIGN

Privacy by Design[11] is an approach that promotes technology design and engineering to incorporate privacy into the design process from the start. The concept includes seven guiding principles on privacy and security.

PSEUDONYMIZATION

For the purposes of this document, pseudonymization means modifying personal data by removing or substituting all direct identifiers (e.g. in many instances name, address, date of birth, etc.) with other unique identifiers (e.g. in many instances hashing algorithms, ID numbers, etc.) in such a way that it is still possible to distinguish a unique individual in a data set. Masking is a type of pseudonymization.

RE-IDENTIFICATION

For the purposes of this document, re-identification means a process by which de-identified (anonymized) data becomes re-identifiable again and thus can be traced back or linked to an individual(s) or group(s) of individuals. As noted in UN Global Pulse Data Innovation Risk Assessment Tool guidance, to determine whether an individual(s) or group(s) of individuals is identifiable, consider all of the means reasonably likely to be used to single out an individual(s) or group(s) of individuals. Factors to consider regarding whether it is reasonably likely that an individual(s) or group(s) of individuals can be re-identified include the required expertise, costs and amount of time required for re-identification, and reasonably and commercially available technology.

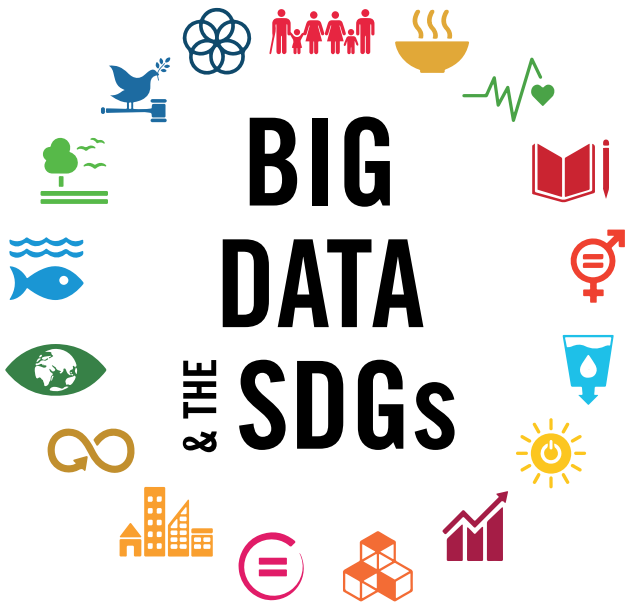
SENSITIVE DATA

For the purposes of this document, sensitive data should be considered as any data related to (i) racial or ethnic origin, (ii) political opinions, (iii) trade union association, (iv) religious beliefs or other beliefs of a similar nature, (v) physical or mental health or condition (or any genetic data), (vi) sexual orientation and other related activities, (vii) the commission or alleged commission of any offence, (viii) any information regarding judicial proceedings, (ix) any financial data, (x) children and (xi) an individual(s) or group(s) of individuals that face any risks of harm (e.g. physical, emotional, economic).

11 The approach was developed by Dr. Ann Cavoukian. A summary is available at https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

ADDENDUM A

HOW DATA ANALYTICS CAN SUPPORT THE SDGS



How data science and analytics can contribute to sustainable development

GLOBAL PULSE

www.unglobalpulse.org
@UNGlobalPulse 2017

1 NO POVERTY
Spending patterns on mobile phone services can provide proxy indicators of income levels

2 ZERO HUNGER
Crowdsourcing or tracking of food prices listed online can help monitor food security in near real-time

3 GOOD HEALTH AND WELL-BEING
Mapping the movement of mobile phone users can help predict the spread of infectious diseases

4 QUALITY EDUCATION
Citizen reporting can reveal reasons for student drop-out rates

5 GENDER EQUALITY
Analysis of financial transactions can reveal the spending patterns and different impacts of economic shocks on men and women

6 CLEAN WATER AND SANITATION
Sensors connected to water pumps can track access to clean water

7 AFFORDABLE AND CLEAN ENERGY
Smart metering allows utility companies to increase or restrict the flow of electricity, gas or water to reduce waste and ensure adequate supply at peak periods

8 DECENT WORK AND ECONOMIC GROWTH
Patterns in global postal traffic can provide indicators such as economic growth, remittances, trade and GDP

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
Data from GPS devices can be used for traffic control and to improve public transport

10 REDUCED INEQUALITY
Speech-to-text analytics on local radio content can reveal discrimination concerns and support policy response

11 SUSTAINABLE CITIES AND COMMUNITIES
Satellite remote sensing can track encroachment on public land or spaces such as parks and forests

12 RESPONSIBLE CONSUMPTION AND PRODUCTION
Online search patterns or e-commerce transactions can reveal the pace of transition to energy efficient products

13 CLIMATE ACTION
Combining satellite imagery, crowd-sourced witness accounts and open data can help track deforestation

14 LIFE BELOW WATER
Maritime vessel tracking data can reveal illegal, unregulated and unreported fishing activities

15 LIFE ON LAND
Social media monitoring can support disaster management with real-time information on victim location, effects and strength of forest fires or haze

16 PEACE, JUSTICE AND STRONG INSTITUTIONS
Sentiment analysis of social media can reveal public opinion on effective governance, public service delivery or human rights

17 PARTNERSHIPS FOR THE GOALS
Partnerships to enable the combining of statistics, mobile and internet data can provide a better and real-time understanding of today's hyper-connected world

BIBLIOGRAPHY

Asia-Pacific Economic Cooperation (2005) APEC Privacy Framework. December. Singapore: APEC Secretariat.

Cavoukian, Ann (2011). Privacy by Design: The 7 Foundational Principles. January. Ontario, Canada: Information and Privacy Commissioner of Ontario.

Council of Europe (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 28 January. ETS No. 108. Strasbourg, Austria.

(1953). European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14. 4 November. ETS 5 (art 8).

Economic Community of West African States (2010). Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS. 16 February.

European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

International Committee of the Red Cross (2015). ICRC Code of Conduct on Data Protection. November. Geneva, Switzerland: ICRC.

International Committee of the Red Cross (2016). ICRC Rules on Personal Data Protection. January. Geneva, Switzerland: ICRC.

International Conference of Data Protection and Privacy Commissioners, Resolution on Data Protection and International Organizations.

International Organization for Migration (2010). IOM Data Protection Manual. Geneva, Switzerland: IOM.

International Organization for Standardization. Online Collection: Information Security Management Systems. Geneva, Switzerland: ISO.

International Telecommunication Union (2015). Recommendation Y.3600. Big data – Cloud computing based requirements and capabilities. 6 November.

Organisation for Economic Co-operation and Development (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 23 September. Paris: OECD.

Organization of American States (1969). American Convention on Human Rights, "Pact of San Jose", Costa Rica. 22 November. Washington, DC: OAS. (art. 11).

United Nations (1989). Convention on the Rights of the Child. Treaty Series 1577 (1989): 3 (art. 16).

United Nations Archives and Records Management Section. Glossary of Recordkeeping Terms.

United Nations Children's Fund (2007). The Paris Principles: Principles and Guidelines on Children Associated with Armed Forces or Armed Groups. February. New York: UNICEF.

United Nations Data Revolution Group (2014). A World that Counts: Mobilising the data revolution for sustainable development. The UN Secretary-General's Independent Expert Advisory Group on a Data Revolution for Sustainable Development. November.

United Nations Development Programme and United Nations Global Pulse (2016). A Guide to Data Innovation for Development – From ideas to proof-of-concept. New York: UN.

United Nations Economic Commission for Europe (2014). The Role of Big Data in the Modernisation of Statistical Production. Geneva, Switzerland: UNECE.

United Nations General Assembly (2016). Quadrennial comprehensive policy review of operational activities for development of the United Nations system. 28 October. A/C.2/71/L.37.

A/70/L.1 (2015). Transforming Our World: the 2030 Agenda for Sustainable Development. 18 September.

A/RES/68/261 from 29 January 2014 (2014). Fundamental Principles of Official Statistics. 3 March.

A/RES/45/158 (1990). International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families (art. 14). 18 December.

A/RES/45/95 (1990).Guidelines for the regulation of computerized personal data files. 14 December.

2200/A (XXI) (1966).International Covenant on Civil and Political Rights. 19 December. UN Treaty Series, vol. 999, No. 14668, p. 171 and vol. 1057, p. 4019 (art. 17).

217 A (III) (1948). The Universal Declaration of Human Rights. 10 December. Paris, France. (art. 12).

Big data for development: Challenges and opportunities, p. 13.

Principles. Data Privacy and Data Protection Principles.

Privacy Tools. Risks, Harms, Benefits Assessment.

United Nations High Commissioner for Human Rights (2016). A Human Rights-Based Approach to Data: Leaving No One Behind in the 2030 Development Agenda, Guidance Note to Data Collection and Disaggregation. 19 February. Geneva, Switzerland; UNHCR.

(2015). Policy on the Protection of Personal Data of Persons of Concern to UNHCR. May. Geneva, Switzerland: UNHCR.

United Nations Human Rights Committee (1988). CCPR General Comment No 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. 8 April.

United Nations Information Security Special Interest Group (June 2013). Use of Cloud Computing in the UN System, Recommendations for Risk Mitigation.

United Nations International Law Commission (2006). Report on the work of the fifty-eight session (2006). Annex IV. Protection of Personal Data in Transborder Flow of Information.

United Nations Statistical Commission (2015). Report of the Global Working Group on Big Data for Official Statistics. 17 December. E/CN.3/2016/6.

United Nations, Human Rights Council (2016). Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. 8 March. A/HRC/31/64, pp. 6, 10. Annex II. A more in-depth look at Open Data & Big Data.

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. 17 April. A/HRC/23/40, p. 6.

World Food Programme (2017). WFP Guide to Personal Data Protection and Privacy. 22 February. Rome: WFP.

World Health Organization (2016). Guidance on Good Data and Record Management Practices. WHO Technical Report Series, No. 996. Annex 5.

UNITED NATIONS DEVELOPMENT GROUP

The United Nations Development Group (UNDG) unites the 32 UN funds, programmes, specialized agencies, departments, and offices that play a role in development. Since 2008, the UNDG has been one of the three pillars of the UN System Chief Executives Board for Coordination, the highest-level coordination forum of the United Nations system.

At the regional level, six Regional UNDG Teams play a critical role in driving UNDG priorities by supporting UN Country Teams with strategic priority setting, analysis and advice.

At the country level, 131 UN Country Teams serving 165 countries and territories work together to increase the synergies and joint impact of the UN system.

The Development Operations Coordination Office (DOCO) is the secretariat of the UNDG, bringing together the UN development system to promote change and innovation to deliver together on sustainable development.