GLOSSARY OF DEFINED TERMS AND ABBREVIATIONS

Anonymization encompasses techniques that can be used to ensure that data sets containing Personal Data are fully and irreversibly anonymized so that they do not relate to an identified or identifiable natural person, or that the Data Subject is not or no longer identifiable.

Artificial Intelligence refers to "[a] set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being".[1] In its current form, it aims to allow technology developers "to entrust a machine with complex tasks previously delegated to a human".[2]

Biometrics or biometric recognition means the automated recognition of individuals based on their biological and behavioural characteristics.

Blockchain is "in essence an append-only decentralized database that is maintained by a consensus algorithm and stored on multiple nodes (computers)".[3]

Cash and Voucher Assistance, Cash Transfer Programming, cash-based interventions and cash-based assistance are terms in the humanitarian sector to describe the delivery of humanitarian aid in the form of vouchers or cash.

CERT – Computer Emergency Response Team

CISO – Chief Information Security Officer

Cloud Services most commonly refers to "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[4]

Consent means the freely given, specific and informed indication of a Data Subject's wishes by which the Data Subject signifies agreement to Personal Data relating to him or her being processed.

CSIRT – Computer Security Incident Response Team

CSO – Chief Security Officer

[1] Council of Europe (CoE), *Glossary on Artificial Intelligence*, Artificial Intelligence, accessed 6 January 2022: www.coe.int/en/web/artificial-intelligence/glossary.

[2] Ibid.

[3] Michèle Finck, "Blockchains and data protection in the European Union", *European Data Protection Law Review*, Vol. 4, No. 1, 2018, p. 17: https://doi.org/10.21552/edpl/2018/1/6.

[4] Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, National Institute of Standards and Technology, US Department of Commerce, Gaithersburg, MD, September 2011: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800–145.pdf.

CTO – Chief Technology Officer

Data Analytics denotes the practice of combining very large volumes of diversely sourced information (big data) and analysing them, using sophisticated algorithms to inform decisions.

Data Breach means the unauthorized modification, copying, unlawful destruction, accidental loss, improper disclosure, or undue transfer of, or tampering with, Personal Data.

Data Controller means the person or organization who alone or jointly with others determines the purposes and means of the Processing of Personal Data.

Data Processor means the person or organization who processes Personal Data on behalf of the Data Controller.

Data Protection Impact Assessment or DPIA means an assessment that identifies, evaluates and addresses the risks to Personal Data arising from a project, policy, programme or other initiative.

Data Subject means a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Personal Data.

Digital Identity refers to "a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions".[5]

DPO in the context of this Handbook means a Humanitarian Organization's internal data protection office or Data Protection Officer.

Drones are small aerial or non-aerial units that are remotely controlled or operate autonomously. They are also known as Unmanned Aerial Vehicles (UAVs) or Remotely Piloted Aircraft Systems (RPAS).

Further Processing means additional Processing of Personal Data that goes beyond the purposes originally specified at the time the data were collected.

Health Data means data related to the physical or mental health of an individual, which reveal information about their health status.

Humanitarian Action means any activity undertaken on an impartial basis to carry out assistance, relief and protection operations in response to a Humanitarian Emergency. Humanitarian Action may include "humanitarian assistance", "humanitarian aid" and "protection".

Humanitarian Emergency means an event or series of events (in particular arising out of armed conflicts or natural disasters) that poses a critical threat to the health, safety, security or well-being of a community or other large group of people, usually over a wide area.

[5] GSMA, World Bank Group, & Security Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, 2016, p. 11: www.gsma.com/mobilefordevelopment/resources/digital-identity-towards-shared-principles-public-private-sector-cooperation/.

Humanitarian Organization means an organization that provides aid to alleviate human suffering, and/or protects life and health, and upholds human dignity during Humanitarian Emergencies in accordance with its mandate and/or mission.

IaaS stands for Infrastructure as a Service.

International Data Sharing includes any act of transferring or making Personal Data accessible outside the country or International Organization where they were originally collected or processed, including to a different entity within the same Humanitarian Organization or to a Third Party, via electronic means, the Internet or other means.

International Organization means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Know Your Customer (KYC) is a process enabling businesses to check the identity of their customers in order to comply with regulations and legislation on money laundering and corruption.[6]

Machine Learning is a specific form of Artificial Intelligence that can be defined as the study of algorithms that improve their performance when completing a certain task with experience in the form of machine-readable data.

PaaS – Platform as a Service

Personal Data means any information relating to an identified or identifiable natural person.

Processing means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, or erasure.

Pseudonymization, as distinct from Anonymization, means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

Reidentification describes the process of turning allegedly Anonymized or Pseudonymized data back into Personal Data through the use of data matching or similar techniques. If the risk of Reidentification is deemed to be reasonably likely, the information should be considered to be Personal Data and subject to all the data

[6] PwC, *Know Your Customer: Quick Reference Guide*, January 2016: www.pwc.lu/en/anti-money-laundering/docs/pwc-kyc-qrg-final-interactive-2016.pdf.

protection principles. It can be very difficult to assess the risk of Reidentification with absolute certainty.

SaaS – Software as a Service

Sensitive Data means Personal Data which, if disclosed, may result in discrimination against or the repression of the individual concerned. Typically, data relating to health, race or ethnicity, religious/political/armed group affiliation, or genetic and biometric data are considered to be Sensitive Data. All Sensitive Data require augmented protection even though different types of data falling under the scope of Sensitive Data (e.g. different types of biometric data) may present different levels of sensitivity. Given the specific situations in which Humanitarian Organizations work and the possibility that some data elements could give rise to discrimination, setting out a definitive list of Sensitive Data categories in Humanitarian Action is not meaningful. Sensitivity of data as well as appropriate safeguards (e.g. technical and organizational security measures) have to be considered on a case-by-case basis.

SLA – A service-level agreement is an official commitment between a service provider and a client, particularly for the provision of reliable telecommunications and Internet services.

Sought Person is a person unaccounted for, for whom a tracing operation has been launched.

Sub-Processor is a person or organization that is engaged by a Data Processor to process Personal Data on its behalf.

Third Party is any natural or legal person, public authority, agency, or any other body other than the Data Subject, the Data Controller or the Data Processor.

TLS – Transport Layer Security is a cryptographic protocol to provide privacy and data integrity between a client and a server over an Internet connection.