DATA PROTECTION GLOSSARY

ACCOUNTABILITY: “the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence … to demonstrate compliance.” *Source: European Data Protection Supervisor*

ACCURATE: Exact, precise, correct; in exact conformity to a standard or to truth. *Source: GBVIMS*

AGGREGATED DATA: Data that has been combined or compiled together thereby becoming anonymous in the process. *Source: GBVIMS*

ANONYMOUS DATA: Data void of information that can be used to identify individuals. *Source: GBVIMS*

CLOUD HOSTING: cloud computing technology allows various machines to act as one system, which is guaranteed by multiple servers. This helps bring efficiencies in web performance, server resources, and data storage. *Source: SiteGround*

CONFIDENTIALITY: The right of every survivor to have their identity kept private and unidentifiable. There is an implicit understanding and obligation on those providing services that any information disclosed by a survivor will not be shared with others, unless the person concerned give explicit and informed consent to do so. Confidentiality involves not only how information is collected, but also how it is stored, and shared. *Source: GBVIMS*

DATA ANALYSIS: is the process by which data or information is aggregated and summarized for presentation. *Source: GBVIMS*

DATA MINIMIZATION: The principle of “data minimization” means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it. *Source: European Data Protection Supervisor*

DATA PROTECTION: Data protection is the act of protecting personal or sensitive information in how it is collected, stored, used, and shared.

DATA SECURITY: “appropriate technical and organizational measures to ensure an appropriate level of security in relation to the risks represented by the processing and the nature of the personal data to be protected. Such measures provide for the prevention of any unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and any other unlawful form of processing.” *Source: European Data Protection Supervisor*

DATA SUBJECT: “The data subject is the person whose personal data are collected, held or processed.” *Source: European Data Protection Supervisor*

DE-IDENTIFIED DATA: Data that cannot be linked to a specific individual or group of individuals by removing all personal identifiers, such as person’s name, place of residence and location. It may be

necessary to consider removing other details to avoid possible identification of a specific individual or group of individuals. *Source: GBVIMS*

INCIDENT: Incident ('violent episode') is defined as an act or series of acts of violence or abuse by one perpetrator or group of perpetrators. May involve multiple types of violence (physical, sexual, emotional, economic, socio-cultural); and may involve repetition of violence over a period of minutes, hours, or days. *Source: GBVIMS*

INFORMATION MANAGEMENT: The manner in which an organization's information is handled or controlled. Includes different stages of processing information including: collection, storage, analysis and reporting/sharing. *Source: GBVIMS*

INFORMATION SHARING PROTOCOL: A document that outlines a set of guidelines for organizations to follow during the information sharing process. *Source: GBVIMS*

INFORMED CONSENT: The approval from a survivor, who is aware of the implications of sharing data on their GBV incident, to share his or her information under certain circumstances. *Source: GBVIMS*

PERSONAL INFORMATION: "any kind of information (a single piece of information or a set of information) that can personally identify an individual or single them out as an individual. The obvious examples are somebody's name, address, national identification number, date of birth or a facial image. A few perhaps less obvious examples include … fingerprints, a computer's IP address, health records. You can be singled out from other people even if your name is not known." *Source: Privacy International*

PURPOSE SPECIFICATION PURPOSE: "the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose." *Source: OECD*

QUALITATIVE: Of or relating to quality or qualities; measuring, or measured by, the quality of something. *Source: GBVIMS*

QUANTITATIVE: That is, or may be, measured or assessed with respect to or on the basis of quantity; that may be expressed in terms of quantity; quantifiable. *Source: GBVIMS*

RELEVANT DATA: Data that can be used for accurate and appropriate data analysis. The tendency is for people to collect more information than they can use, and in a level of detail that limits its utility to produce general statistics and meaningful data analysis. *Source: GBVIMS*

SECURITY SAFEGUARDS PRINCIPLE: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data." *Source: OECD*

USE LIMITATION: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject and as legal *Source: OECD*