GLOSSARY OF TERMS

1.Introduction

Motus processes data which must be governed, managed and used in accordance with the policies, procedures, standards and guidelines developed by Motus.

2.Purpose

2.1 The purpose of this Glossary is to provide a guide for the consistent use of words, phrases and abbreviations in the policies, procedures, standards and guidelines developed by Motus.

2.2 This Glossary is a "living document" which should be updated regularly to promote a consistent understanding of words and phrases used in policies, procedures, standards and guidelines, which reflect their usage and understanding within Motus and to add or amend the definition of terms as may become necessary.

2.3 This Glossary is supplemented by Technical Abbreviations relevant to Motus information and communications technologies (ICT), that may be used in the development of policies, procedures, standards and guidelines.

2.4 This Glossary is supplemented by Technical Abbreviations relevant to Motus information and communications technologies (ICT), that may be used in the development of policies, procedures, standards and guidelines.

3.Audience

This Glossary applies to the drafters of all policies, procedures, standards or guidelines addressing data processed by Motus.

4.Glossary of terms

4.1 Words and phrases defined below shall, unless the context in which it is used is clearly contrary to this Glossary, bear the meaning attributed to the word or phrase contained in this Glossary.

4.2 Capitals are not used to represent defined words or phrases unless language usage dictates or specifically required by Motus.

4.4 Capitals are used in abbreviations unless custom or language usage dictates the contrary.

4.5 In some instances, the term defined is also defined in relevant legislation of regulation. For the purposes of convenience and ease of reading the term referred to in legislation or regulation will not be used in full but a reference to the definition in the legislation or regulation will be provided in bold after the definition.

Term Definition Abbreviation

Biometrics: Means a technique of personal identification that is based on physical, physiological or behavioral characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

Child: Means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him-or herself.

Competent person: Means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

Consent: Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information.

Control: Means any administrative, management, technical or legal method that is used to manage risk. Controls are safeguards or countermeasures. Controls include things like practices, policies, procedures, programs, techniques, technologies, guidelines and organizational structures.

Data: Means any recorded data, regardless of the medium used to record the data, used by Motus in the conduct of its business. Data may be used interchangeable with "information".

Data Class: Means the classification of the particular type of data into one of four categories, being Public, Operational, Personal or Confidential.

Data subject: Means the person to whom Personal Information relates.

Information: Means any recorded information, regardless of the medium used to record the information, used by Motus in the conduct of its business. Information may be used interchangeable with "data".

Information and Communications Technologies: Means Information technologies including, without limitation, the Internet, wireless networks, cellular phones, mobile communication devices and other communications mediums.

ICT Information Officer: Means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act being the Chief Executive Officer or equivalent officer of the juristic person or any person duly authorised by that officer; or the person who is acting as such or any person duly authorised by such acting person;

IO Operator: Means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

Person: Means a natural person or a juristic person.

Personal Information Breach: Means a breach of security leading to the accidental or unlawful damage to, destruction, loss, alteration, unauthorised or unlawful disclosure of, or access to, Personal Information.

POPIA: Means the Protection of Personal Information Act, 2013, and any and all regulations and codes of conduct promulgated or issued pursuant thereto, in each case as amended from time to time;

Processing, Processes and Process: Means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including: · The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use. · Dissemination by means of transmission, distribution or making available in any other form. · Merging, linking, as well as restriction, degradation, erasure or destruction of information.

Public record: Means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

Record: Means any recorded information.

Responsible party: Means a public or private body or any other person who, alone or in conjunction with others, determines the purpose of and means for processing personal information.

Personal Information: Means any information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, that is processed by the Service Provider for the client, including but not limited to: · information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person; · information relating to the education or the medical, criminal or employment history of the person; · financial information of the person, including but not limited to, salary details and financial commitments and information relating to the financial history of the person. · information of the vehicle and vehicle service history of the person. · any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person. · the biometric information of the person. · the personal opinions, views or preferences of the person. · correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence. · the views or opinions of another individual about the person; and · the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Technical and Organisational Security Measures'

Means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

The Data Exporter

Means the controller who transfers the personal data;

The Data Importer

Means the processor who agrees to receive from the data

The Subprocessor

Means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract.

5.Technical Abbreviations

Abbreviation Definition

AAL: Authenticator Assurance Level (AAL). A category describing the strength of the authentication process.

AAL2: AAL2 provides high confidence that the claimant controls authenticator(s) bound to `the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.

AAL3: AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication SHALL use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device MAY fulfil both these requirements. In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

AES 128: Advanced Encryption Standard, is a specification for the encryption of electronic data.

ASCII : Abbreviated from American Standard Code for Information Interchange, is a character encoding standard for electronic communication. ASCII codes represent text in computers, telecommunications equipment, and other devices.

CSP: Credential Service Provider. A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or issue credentials for its own use.

DDoS: A type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.

DKIM: Domain Keys Identified Mail (DKIM) is an email authentication method designed to detect forged sender addresses in emails, (email spoofing), a technique often used in phishing and email spam.

DLP: Data Loss Prevention. A strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

ECDH: (For agreeing session keys). An anonymous key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel.

ECDSA: Elliptic Curve Digital Signature Algorithm.

FAL: Refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).

FAL2: Encryption using approved cryptography such that the RP is the only party that can decrypt it.

FAL3: Requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artefact itself. The assertion is signed by the IdP and encrypted to the RP using approved cryptography.

IAL: Identity Assurance Level. A category that conveys the degree of confidence that the applicant's claimed identity is their real identity.

IAL2: Introduces the need for either remote or physically present identity proofing.

IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the Credential Service Provider.

IDP: The party that manages the subscriber's primary authentication credentials and issues assertions derived from those credentials. This is commonly the CSP as discussed within this document suite.

IEEE 1394: An interface standard for a serial bus for high-speed communications and isochronous realtime data transfer.

RP: Relying Party. An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

S/MIME 3.2: MIME (Multi-Purpose Internet Mail Extensions) is an extension of the original Internet e-mail protocol that lets people use the protocol to exchange different kinds of data files on the Internet: audio, video, images, application programs, and other kinds, as well as the ASCII text handled in the original protocol, the Simple Mail Transport Protocol (SMTP).

SHA-384: Secure Hash Algorithm.

SSH Protocol 2: SSH provides a secure channel over an unsecured network in a client–server architecture, connecting an SSH client application with an SSH server.

TLS v1.2: Transport Layer Security – TLSv1.2. Currently TLSv1.2 is the newest SSL protocol version. It introduces new SSL/TLS cipher suites that use the SHA-256 hash algorithm instead of the SHA-1 function, which adds significant strength to the data integrity. TLSv1.2 is supported with OpenSSL 1.0.1e or later