AUDA-NEPAD
AFRICAN UNION DEVELOPMENT AGENCY

STANDARD OPERATING PROCEDURE

Protection of Personal Data Standard Operating Procedures

1. Introduction

In 2014, African Union (AU) Member States adopted the African Union Convention on Cyber Security and Personal Data Protection. The adoption and subsequent ratification of the Convention on CSPD by most Member States sets a strong objective of African action on cybersecurity and personal data protection to deliver benefits to Africa. To facilitate the implementation of the Legal Framework for Cyber Security and Personal Data Protection (CSPDP) African Union Development Agency (AUDA–NEPAD) has developed the standard operating procedures to assist in the implementation, specifically on the Personal Data Protections (PDP)

The standard operating procedure lay down rules relating to the protection of natural persons about the processing of personal data and rules relating to the free movement of personal data. The SOP guides individuals on how to take a more active role in the protection of their personal data, while recognising the responsibility of AUDA – NEPAD for a positive outcome in the protection of personal data.

Privacy and Personal Data Protection is a broad and ever-changing domain; the SOP is not an end-state they are a blueprint for an evolving practice as new circumstances and requirements emerge. The SOP will be subject to review annually and additionally in response to any changes affecting the basis of the original document. The SOP will also be reviewed to monitor its effectiveness, demonstrated by the nature, number and impact of recorded incidents.

2. Rationale

Information is an asset which, like other important business assets, has value to an organisation and consequently needs to be suitably protected. Processing and transmission of personal data on Individuals who can be identified from the information has legislative controls placed on them. The objective of this document is to provide management direction and support for data protection.

AUDA–NEPAD is often required to process personal data of persons of concern to the Organization. This includes sharing of personal data with Implementing Partners and other stakeholders. In processing personal data there are inherent risks such as accidental or unauthorized loss or disclosure. Given the particularly vulnerable position of persons of concern to AUDA–NEPAD, the nature of their personal data is generally sensitive and, therefore, requires careful handling in line with this SOP. For AUDA–NEPAD, proper protection of the personal data of persons is important.

3. Compliance and supervision of compliance

The Data Protection Procedure have several measures to ensure compliance and supervision of compliance, including:

(i) The appointment of one Data Protection Officer to oversee and supervisee AUDA–NEPAD's compliance.

(ii) Each directorate and Business Unit to identify an officer as appropriate, who will be responsible for the supervision and overseeing of data protection compliance during and after meetings, conferences, and events where personal data such as collection of passports for processing Of DSA's is conducted; and

(iii) Establishment of internal control mechanisms and ongoing monitoring.

4. Scope

The SOP applies to all personal data held by AUDA–NEPAD in relation to persons of concern to AUDA–NEPAD. This SOP does not cover processing of data such as

(i) by a natural person during a purely personal or household activity,
(ii) by competent authorities 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.

5. Terms and Definitions

1)	Biometric data	Means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data;
2)	Consent	Means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
3)	Data Breach	A breach of data security leading to the accidental or unlawful/ illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transferred, stored or otherwise processed.
4)	Data controller	The AUDA-NEPAD staff member who has the authority to oversee the management of, and to determine the purposes for the processing of personal data.
5)	Data Subject	An individual whose personal data is subject to processing.
6)	Data Transfer Agreement	An agreement between AUDA-NEPAD and an Implementing Partner or third party that states the terms and conditions of use of personal data, including which data components are to be shared, the mode of transfer, how the data may be used, data security measures and other related issues.
7)	Filling System	'Filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional basis.
8)	Implementing Partner	An organization established as an autonomous and independent entity from AUDA-NEPAD that AUDA-NEPAD engages through Grants of Sub delegation or project partnership agreement to undertake the implementation of programmatic activities within its mandate.
9)	Personal data	Means any information relating to an identified or (directly or indirectly) identifiable natural person. Personal data includes biographical data (biodata) such as name, sex, marital status, date and place of birth, country of origin, individual registration number, occupation, religion, and ethnicity, biometric data such as a photograph, fingerprint, facial or iris image, as well as any expression of opinion about the individual, such as assessments of the status and/or specific needs
10)	Personal Data Breach	personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
11)	Processor	'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
12)	Profiling	'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person to analyse or predict aspects concerning that natural person's performance at work, economic situation, health,

	personal preferences, interests, reliability, behaviour, location, or movements;
13) Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
14) Pseudonymisation	pseudonymisation' 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
15) Third Party	Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of AUDA NEPAD are authorised to process personal data

6. Principles of Personal Data Processing

Article 13 of the African Union Convention on Cyber Security and Personal Data Protection has identified the following principles relating to data protection.

(a) Consent and legitimacy of personal data processing,
(b) Lawful and fair processing of personal data processing,
(c) Purpose, relevance and storage of processed personal data,
(d) Accuracy of personal data,
(e) Transparency of personal data processing, and
(f) Confidentiality and security of personal data processing.

Consent and Legitimacy

Processing of personal data shall be deemed to be legitimate where the data subject has given consent. The requirement of consent may be waived under the following conditions where processing is necessary for:

(a) Compliance with a legal obligation to which the controller is subject.
(b) Performance of a task carried out in the public interest or in the exercise of official authority.
(c) Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject to entering a contract.
(d) Protect the vital interest of fundamental rights and freedoms of the data subject

Lawful and fair processing of personal data processing

The collection, recording, processing, storage and transmission of personal data shall be undertaken lawfully, fairly and non-fraudulently, as per para (6.1) above and if the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject.

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person.
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Purpose, relevance and retention of data

(a) Personal data must be collected only for specified, explicit, and legitimate purposes.
(b) Personal data should only be used for such other purposes as are compatible with those purposes;
(c) Data collection shall be in accordance with applicable laws, such as archiving data that is in the public interest, or for scientific research.
(d) Be adequate , relevant and not excessive in relation to the purpose for which they are collected and further processed;
(e) Data shall be kept for no longer than necessary for the purposes for which the data were collected or further processed;
(f) Beyond the required period, data may be stored only for specific needs of data processing undertaken for historical, statistical or research purposes under the law.

Accuracy of personal data over its lifespan,

Personal data shall be recorded as accurately as possible and, where necessary, updated to ensure it satisfies the purpose(s) for which it is processed.

Transparency of processing

The principle of transparency requires mandatory disclosure of information on personal data by AUDA–NEPAD.

Confidentiality and security of personal data.

AUDA–NEPAD personnel shall always maintain the confidentiality of the personal data of persons of concern even after a data subject is no longer with the organisation. All members of staff irrespective of their involvement in processing and protection of data, shall sign 'declaration of confidentiality'. To ensure confidentiality and integrity of personal data, appropriate technical and organizational data security measures shall be enshrined in the Data Management Policy.

Security of processing

Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data.
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken of the risks that are presented by processing, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller unless he or she is required to do so by law.

Accountability.

Those who collect and process personal data must be able to demonstrate their compliance with these principles.

7. Respect for the data subject's Rights

Information to be provided where personal data are collected from the data subject

AUDA–NEPAD shall provide the natural person whose data are to be processed, no later than the time when the data are collected, regardless of the means and facilities used, with the following information:

(a) His/her identity and of his/her representative, if any,
(b) The purpose of the processing for which the data are intended.
(c) Categories of data involved.
(d) Recipient(s) to which the data might be disclosed.
(e) The capacity to request to be removed from the file.
(f) Existence of the right of access to and the right to rectify the data concerning him/her.
(g) Period for which data are stored.
(h) Proposed transfers of data to third parties.

Right of access by the data subject

Upon request the data subject may receive from AUDA–NEPAD:

(a) Such information as would enable him/her to evaluate and either agree or object to the processing.
(b) Confirmation as to whether data relating to him/her are being processed.
(c) Communication to him/her of the personal data undergoing processing and any available information to their source
(d) Information as to the purpose of processing, the categories of personal data concerned, and the recipients or categories of recipients to who the data are disclosed.
(e) The right to obtain a copy referred to in this paragraph shall not adversely affect the rights and freedoms of others

Right of rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Considering the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure (Right to be forgotten)

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise Processed.
(b) the Data Subject withdraws his or her Consent to the Processing and where there is no other legal basis for the Processing.
(c) the Data Subject objects to the Processing pursuant to the processing of the Personal Data and there are no overriding legitimate grounds for the Processing,
(d) the Personal Data have been unlawfully Processed.

(e) the Personal Data must be erased in compliance with a legal obligation on the applicable law to which the Controller is subject.

Right to object

A data subject may object to the processing of his or her personal data where there are legitimate grounds related to his or her specific personal situation. If the objection is justified, AUDA–NEPAD is under the obligation d not to proceed with the l processing of the personal data concerned.

Right to data portability

The purpose of the right to data portability is to promote interoperability between systems and to give greater power to the data subjects over the data that AUDA – NEPAD hold and an increased level of control and choice.

The data subject has the right to request a copy of all personal data that AUDA–NEPAD holds on his or her behalf. This must then be transmitted directly from AUDA–NEPAD in a manner that will easily allow the data subject further access to use of the data.

Data portability means data that can be received by the data subject in a structured or commonly used machine-readable format and have the right to transmit those data to another controller without hindrance and restrictions generated by AUDA–NEPAD systems.

Right to Confidentiality of electronic communications

All users of electronic mail are informed about the confidentiality, privacy, and security applicable to electronic mail. Information should be classified according to an appropriate level of confidentiality, integrity and availability pursuant to the ICT Policy.

Members of AUDA–NEPAD will have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of information. These include:

Heads of divisions, units

Responsible for the information systems (e.g., HR/Registry/Finance) both manual and electronic that support AUDA–NEPAD work.

Divisional managers/Line managers

Responsible for specific areas of AUDA-NEPAD work, including all the supporting information and documentation that may include working documents, contracts, staff information.

Consultants/third parties/Sub-Contractors

Responsible for the security of information produced, provided, or held while carrying out research, consultancy, or knowledge transfer activities. This includes ensuring that data is appropriately stored; that the risks to data are appropriately understood and either mitigated or explicitly accepted; that the correct access rights have been put in place with data only accessible to the right people; and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.

8. Data Processing by AUDA-NEPAD

Confidentiality of personal data

Personal data is classified as confidential. Activities related to the collection and use of data shall be consistent with applicable confidentiality, privacy, and other regulations. (Refer to Data Policy). The confidentiality of personal data must always be respected by AUDA–NEPAD when processing personal data.

To ensure and respect confidentiality, personal data must be filed and stored where it is accessible only to authorized officers and transferred only using protected means of communication.

Security of personal data

AUDA–NEPAD shall use any means available to protect its data from risks presented by the nature and processing of personal data, by making available very good quality of the necessary equipment, the cost and the operational feasibility. One of the functions of the Information Technology Unit shall be Data Security.

AUDA–NEPAD's data security measures are to protect personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This SOP shall be read together with IT Policies on security of data.

To ensure the security of AUDA–NEPAD information, the configuration of the personal devices to access AUDA–NEPAD information shall only be done by MIS. All users whose personal devices have camera, video or recording capability are restricted from using those functions in areas restricted by AUDA–NEAPD Security. Where recording is necessary a privacy note shall be sent to all attending for endorsement before such recording can be seen as legal..

Having regard to available technologies, AUDA–NEPAD shall take measures to ensure the implementation of data protection enhancing technologies and tools to enable data processors to better protect personal data. These may include:

Ensuring accuracy of personal data

Data quality is multi-dimensional, and involves data management, modelling and analysis, quality control and assurance, storage and presentation. Data quality is related to use and cannot be assessed independently of the user.

AUDA–NEPAD may correct or delete personal data held in its systems that is inaccurate, incomplete, unnecessary or excessive. To maintain accuracy AUDA–NEPAD shall update personal data records when necessary and periodically verify them.

It is the responsibility of all data users to verify data they use. However, to ensure data quality the delegated data owner (business unit, or project) must certify the quality of data being processed for the use of the AUDA-NEPAD through appropriate data collection mechanisms followed by data validation and verification.

When personal data is corrected or deleted in AUDA–NEPAD 's systems, AUDA–NEPAD should notify, as soon as reasonably practicable, all Implementing Partners and/or third parties.

Notification of a personal data breach

Data is one of AUDA-NEPAD's most important assets. In order to protect this asset from unauthorized use, loss or destruction, it is imperative that it is safely and securely captured, copied, and stored. Any security breach of AUDA–NEPAD information systems could lead to possible loss of confidentiality, integrity and availability of personal or other confidential data stored in the information systems.

Loss or breach of confidentiality of contractually assured information may result in financial penalties and criminal or civil action. Therefore, it is crucial that all users of the AUDA–NEPAD information systems adhere to the Information Security Policy and its supporting policies.

All AUDA–NEPAD staff and other authorised users should be informed of all policies and regulation on protection of personal data. Any security breach is handled in accordance with all relevant AUDA–NEPAD policies, including the conditions on usage of ICT facilities.

System administrator is responsible for notifying the designated information owner, if they suspect a user is responsible for misusing the information system or is in breach of the IT Policy. AUDA-NEPAD personnel are required to notify the Systems administrator or the Human Resources division as soon as possible upon becoming aware of a personal data breach and to properly record the breach.

If personal data breach is likely to result in personal injury or harm to a data subject, the data controller designate should use his or her best efforts to communicate the personal data breach to the data subject and take mitigating measures as appropriate without undue delay. In such cases, MIS and the Human Resources Division should be notified.

The notification should describe:

(a) The nature of the personal data breach, including the categories and number of data subjects and data records concerned.
(b) The known and foreseeable adverse consequences of the personal data breach; and
(c) The measures taken or proposed to be taken to mitigate and address the possible adverse impacts of the personal data breach.

Data retention

Personal data that is not recorded in individual files is not to be retained longer than necessary for the purpose(s) for which it was collected. All individual case files, whether open or closed, are considered permanent records, and must therefore be permanently retained in line with the Archiving requirements.

Joint controllers

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by the African Union Statutes to which the controllers are subject.

The arrangement may designate a contact point for data subjects. The arrangement referred to in paragraph above shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject. Irrespective of the terms of the arrangement referred to above, the data subject may exercise his or her rights in respect of and against each of the controllers.

9. Data processing by third parties

Third Party

Third party, in relation to personal data, means any person other than: AUDA–NEPAD, Data subject or any data processor or other person authorised to process data for AUDA – NEPAD. The expression third party does not include employees or agents of AUDA – NEPAD. If collection and processing of personal data is one of the responsibilities of Implementing Partners, the personal data being collected and processed on behalf of AUDA -NEPAD. For these reasons, Implementing Partners are expected to respect and implement the same or comparable standards and basic principles of personal data protection and in accordance with their professional regulations

Verification

AUDA–NEPAD shall verify prior to transferring personal data to an Implementing Partner or to engaging an Implementing Partner in the collection and processing of personal data, that the processing of personal data by the Implementing Partner satisfies the standards and basic principles adapted by AUDA–NEPAD. Verification shall be undertaken, in the form of assessment of the implementing partner, when conducting TOCA.

The data subject should be informed, about the transfer of his/her personal data.

Third Party Agreements/Contracts

The Implementing Partners to comply with the protection of personal data through an undertaking as part of the signing of partnership agreements. Such agreements also need to stipulate the specific purpose(s) for the processing of personal data and the legitimate basis for processing.

The contractual relationship between AUDA–NEPAD and its implementing partners also entails the responsibility upon AUDA–NEPAD to verify that the processing of personal data by the implementing partner, economic operators satisfies the African Union Convention on Cyber Security and Protection of Personal Data protection standards and principles and ensure that implementing partners have the necessary capacity to comply. (due diligence)

After termination of the agreement or the contract, all personal data collected during the performance of the partnership would be returned to AUDA–NEPAD. Partnership agreements may provide for exceptions, where there are legitimate reasons to do so, namely consent of the data subjects

The third party respects the confidentiality of personal data transferred to them by AUDA-NEPAD. Whether or not a data transfer agreement has been signed between AUDA–NEPAD and the third party. AUDA – NEPAD must include a confidentiality clause in all its contracts.

Transfer of personal data to third parties

AUDA–NEPAD need to ensure that transferring personal data does not negatively impact:

(a) the safety and security of AUDA–NEPAD personnel and/or personnel of Implementing Partners;
(b) the effective functioning of an AUDA–NEPAD operation or compromise AUDA–NEPAD's mandate, due to the loss of trust and confidence.

Before agreeing to transfer personal data to a third party, AUDA–NEPAD need to assess the level of data protection afforded by the third party. As part of this assessment, the data controller should assess, inter alia, the applicable regulations, internal statute and policies of the third party, specific contractual obligations or undertakings to respect specific data protection frameworks, their effective implementation as well as the technical and organizational means of data security put in place.

Annex

Data Transfer Agreement (DTA)

This template is to be used to govern the transfer of personal data. It is designed for cases, where no cooperation agreement exists.

1. Party	The undersigned, the provider [name of legal entity], incorporated, organized and duly existing under the laws of the [name of jurisdiction], with its principal office at [insert address], hereby legally represented by [insert name of legal representative] have agreed to be bound by the provisions set out in this agreement
2. Scope	AUDA– NEPAD provides to the Recipient the following data: [fill in precisely or point to an attachment where the provision is described]. The Recipient acknowledges that the data are provided on an "as is" basis without any warranty of satisfactory quality or fitness for a particular purpose or use or any other warranty, express or implied.
3. Data Protection	a) AUDA–NEPAD confirms that for the purposes of this DTA it is entitled to provide the data to the Recipient and that consent covering the intended use has been obtained from the relevant data subjects. b) The Recipient will use data for purposes of [*Indicate intended purpose]*. The Recipient confirms that the intended use has been approved by AUDA–NEPAD. c) The Recipient confirms that all work using the data will be carried out in compliance with all applicable laws, professional regulations, guidelines and approvals. d) The Recipient will retain the data in a secure network system at such standard as would be reasonably expected for the storage of valuable and proprietary for sensitive OR confidential data. e) The Recipient shall refrain from tracing or identifying the identity of any data subject who provided the data. Recipient agrees to preserve, always, the confidentiality of information pertaining to data subjects. f) The Recipient agrees not to give access to data, in whole or part, or any identifiable data derived from the data, to any third party. g) The Recipient shall limit access to and processing of the data to those employees or other authorized representatives of Recipient who: (i) need to process such data in order to conduct their work in connection, (ii) have signed agreements with the Recipient

	obligating them to maintain the confidentiality of the data and any information to be derived thereof or disclosed to them. h) Recipient shall take reasonable steps to delete data for a given subject when the provider deems that subject to have withdrawn his or her consent. i) The Recipient confirms that it will deal promptly and appropriately with any withdrawals by data subjects which AUDA–NEPAD Provider notify to the Recipient, j) Any provisions of this agreement intended to protect the human rights of the data subjects shall survive the expiry or termination of this agreement
4. Intellectual Property	(a) Title to the data is and remains in the property of the AUDA–NEPAD. (b) To the extent that AUDA–NEPAD and the Recipient have each contributed to an invention with respect to the material, they shall jointly own any rights to such an invention.
5. Credits	(a) The Recipient agrees to acknowledge the source of the data in any publications or other public disclosures reporting use of it. The following form of words should be used: "We acknowledge AUDA–NEPAD, funded by [..] for the supply of the Data".
6. Reports	(a) The Recipient shall provide a copy of any report of its Results that derive from use of the resource to the Provider in any format (e.g. paper journal, on-line report, meeting abstract). (b) Notices required under this DTA will be in writing and will be delivered by email to the addresses set out below or (in the event of a failure to deliver an email) by post to the Provider or the Recipient and will be deemed to be given, in the case of delivery by email, upon receipt at the Recipient 's email server (unless an automatic response indicating an undeliverable message is received) and, in the case of delivery by post, on the date of delivery (or, if not a business day, on the first business day thereafter).
7. Expiry/Termination	(a) This agreement shall expire [fill in date], unless earlier terminated by the mutual written agreement of the parties. (b) The Provider will be entitled to terminate this DTA forthwith by written notice to the Recipient if: • The Recipient commits any breach of a data provision of this DTA and, in the case of a breach capable of remedy, fails to remedy the same within 20 days after receipt of a written notice giving particulars of the breach and requiring it to be remedied;

	• a breach will be considered capable of remedy if the Recipient can comply with the provision in question in all respects other than as to the time of performance, if time of performance is not of the essence, • The Recipient Institution ceases, is likely to cease, or threatens to cease carrying on business. (c) Upon expiry or termination of this Agreement: • The grant of rights to the Recipient will be automatically terminated; • The Recipient shall delete the data.
8. Assignment and sub-contracting	(a) Neither party will be entitled to assign this DTA or any of its rights or obligations hereunder without first having received the written approval of the other party, which approval not to be unreasonably withheld or delayed. (b) The Recipient will not sub-contract the performance of any of its obligations under the DTA or any part thereof without having first obtained the prior written consent from AUDA – NEPA. In the event that consent is granted, the Recipient shall be responsible for the acts, defaults and omissions of its sub-contractors as if they were the Recipient's own, and any consent given will not relieve the Recipient of any of its obligations under this DTA.
9. Applicable law and jurisdiction	(a) This DTA will be governed by and construed in accordance with the standard operating procedures of the AUDA-NEPAD data protection.
10. Force majeure	(a) If any party is prevented from, hindered or delayed in performing any of its obligations under this DTA by reason of a Force Majeure Event, such party will promptly notify the other of the date of its commencement and the effects of the Force Majeure Event on its ability to perform its obligations under this DTA. (b) If mutually agreed by the parties, then the obligations of the party so affected will thereupon be suspended for so long as the Force Majeure Event may continue. The party affected by a Force Majeure Event will not be liable for any failure to perform any of its obligations as are prevented by the Force Majeure Event provided that such party will use every reasonable effort to minimise the effects thereof and will resume performance as soon as possible after the removal of such Force Majeure Event. (c) If the period of non-performance exceeds 28 days from the start of the Force Majeure Event then the non-affected party will have the option, by written notice to the other party, to terminate this DTA. (d) For the purpose of this clause, Force Majeure Event means any event beyond the reasonable control of a party including, without limitation, acts of God, war, terrorism, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, fire, flood or storm.

	For the avoidance of doubt, strike, industrial action, failure of technology systems, third party insolvency and failure of the Provider or any other third party will not be considered to be Force Majeure Events.
11. Limitation of Liability and Indemnity	(a) The Recipient will indemnify AUDA–NEAPD against all losses (whether direct or indirect, reasonably foreseeable or specifically contemplated by the parties), damages, costs, expenses (including but not limited to reasonable legal costs and expenses) that it incurs as a result of: (i) the use, storage or disposal of human personal data by the Recipient; or (ii) any negligence or wilful default of the Recipient, provided that the Provider agrees to use its reasonable endeavours to mitigate any loss.
12. Variations	(a) All variations to this DTA must be agreed, set out in writing and signed on behalf of the parties before they take effect.