DATA POLICY, REGULATORY FRAMEWORK, AND CYBERSECURITY

TABLE OF CONTENTS

01

INTRODUCTION

- Data & Cybersecurity – overview of general national approaches
- Data & Cybersecurity – overview of Africa’s general approach

02

DATA & CYBERSECURITY IN SPACE

- At the International level
- At the Continental level
- At the National level

03

RECOMMENDATIONS

01 INTRODUCTION

1.1

INTRODUCTION

DATA & CYBERSECURITY
OVERVIEW OF GENERAL NATIONAL APPROACHES

Data & Cybersecurity – overview of general national approaches

DATA

Data economy

Data sharing B2G and G2B

Big Data

- Protection: IP/database laws
- Flows: Free-flow across borders (and freedom of information)

Data privacy

Personal data

- Protection: personal data laws
- Flows: International transfers

CYBERSECURITY

Security of network and information systems

- Cybersecurity obligations – CIA
- Notification of incidents

Critical infrastructure

- Security obligations
- Specific contact points

Sector/area-specific, e.g.

- Electronic communications
- Fintech
- Personal data

Cybercrime

1.2

INTRODUCTION

DATA & CYBERSECURITY
OVERVIEW OF AFRICA’S GENERAL APPROACH

Data & Cybersecurity – overview of Africa's general approach

AFRICAN UNION CONVENTION

Malabo Convention

Adopted in 2014 and signed or ratified by 22 out of 54 African countries

Stems from African commitment towards a digital society and is aimed at a joint recognition of the need to protect critical cyber/ICT infrastructure, personal data and to encourage information flow towards an adequate digital space in Africa

Convention handles:

- E-commerce
- Institutional framework for data protection
- State commitment towards fostering a cyber security culture

Intended to be followed by each member-state approving national legislation based on the principles of the Convention

ITU / INTERNET SOCIETY

Data Protection Guidelines for Africa

- Created to facilitate the implementation of the Convention
- Sets 18 recommendations aiming to create trust, privacy, and responsible use of personal data
- Generally based on EU Directive pre-GDPR

Data & Cybersecurity – overview of Africa's general approach

Southern Africa Development Community

- **SADC Model Law**
- Community with 16 Sub-Saharan member states
- Model law was prepared and adopted in 2013 with the assistance of the EU, with co-funding through the 9th European Development Fund (EDF) and generally based on EU Data Protection Directive
- Aimed at being approved by SADC member states at a national level

Economic Community of West African States

- **ECOWAS Data Protection Act**
- Community with 15 member states
- General template based on EU's pre-GDPR approach and approved in 2010
- Aimed at providing data protection legal background for ECOWAS members without specific legislation in this respect

East African Community

- **East African Community Cybercrime Framework**
- Community with 6 member states
- Calls for member states to enact laws on cybercrime

02 DATA & CYBERSECURITY IN SPACE

2.1 DATA & CYBERSECURITY IN SPACE

AT THE INTERNATIONAL LEVEL

Data

UNITED NATIONS
Remote Sensing Principles

- Right of sensed State to non-discriminatory access to data and analysed information
- Duty of the sensing State to make data available to sensed State, especially for disasters
- Promote international cooperation

Data

PLATFORMS AND PROGRAMMES

United Nations (UNOOSA)

UN-SPIDER – United Nations Platform for Space-based Information for Disaster Management and Emergency Response

17 space agencies

Space & Major Disasters Charter

European Union

Copernicus Programme

UN-GGIM
(UN Initiative on Global Geospatial Information Management)

ORGANISATIONS

GEO
Intergovernmental Group on Earth Observations

CEOS
Committee on Earth Observation Satellites

Cybersecurity

UNITED NATIONS

- **UN Space Treaties**: no cybersecurity obligations, but there are provisions the compliance of which may require the implementation of security measures within satellite systems. E.g. non-contamination / debris
- **Guidelines for the Long-term Sustainability of Outer Space Activities** – no express reference to cybersecurity
- **TCBMs**: e.g., exchanges of information on forecast natural hazard in outer space, notification in the case of emergency situations – no express reference to cybersecurity

Cybersecurity

Some Initiatives

- **United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security** deals with existing and potential threats in the sphere of information security, as well as possible cooperative measures to address them

- **ITU-IMPACT –** ITU International Multilateral Partnership against Cyber Threats (IMPACT) is a cybersecurity alliance and public-private partnership that works to address and prevent cyber threats

2.2

DATA & CYBERSECURITY IN SPACE

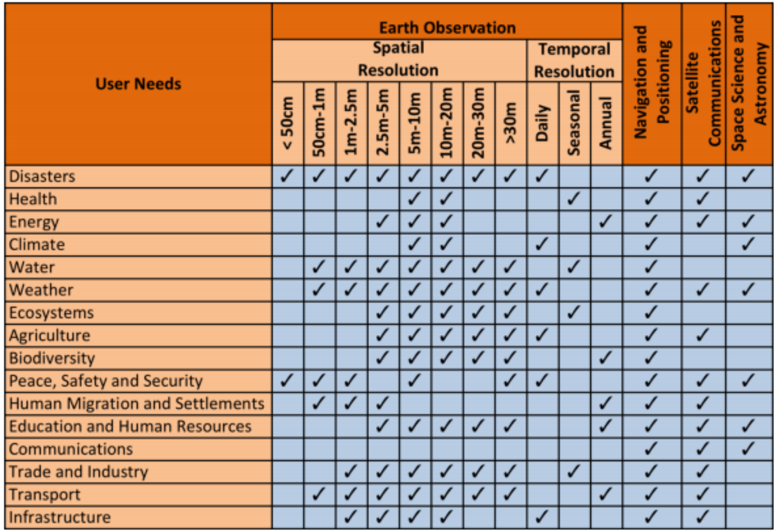
AT THE CONTINENTAL LEVEL

African Union

African Space Policy and Strategy

Importance of EO is mentioned, including:

- Build capabilities in Earth observation systems
- Develop skills and expertise in Earth observation applications and usage
- Develop and improve Earth observation institutions in Africa
- Foster knowledge sharing
- Develop space-based and in-situ infrastructure
- Develop Earth observation services and products
- Raise awareness among the public, users, and policy and decision maker



User Needs	Earth Observation											Navigation and Positioning	Satellite Communications	Space Science and Astronomy
	Spatial Resolution								Temporal Resolution					
	< 50cm	50cm-1m	1m-2.5m	2.5m-5m	5m-10m	10m-20m	20m-30m	>30m	Daily	Seasonal	Annual			
Disasters	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓
Health					✓	✓				✓		✓	✓	
Energy				✓	✓	✓					✓	✓	✓	✓
Climate					✓	✓			✓			✓		✓
Water		✓	✓	✓	✓	✓	✓	✓		✓		✓		
Weather		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓
Ecosystems				✓	✓	✓	✓	✓		✓		✓		
Agriculture				✓	✓	✓	✓	✓	✓			✓	✓	
Biodiversity				✓	✓	✓	✓	✓			✓	✓		
Peace, Safety and Security	✓	✓	✓		✓			✓	✓			✓	✓	✓
Human Migration and Settlements		✓	✓	✓							✓	✓	✓	
Education and Human Resources				✓	✓	✓	✓	✓			✓	✓	✓	✓
Communications												✓	✓	✓
Trade and Industry			✓	✓	✓	✓	✓	✓		✓		✓	✓	
Transport		✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	
Infrastructure			✓	✓	✓	✓			✓			✓	✓	

Projected 10-year outcomes

- Independent Earth observation high-resolution satellite data available for all of Africa from a constellation of satellites designed and manufactured in Africa

No express reference to cybersecurity beyond reference to the Convention on Cyber Security and Personal Data Protection

African Union

ORGANISATIONS

Under the auspices of UNECA

- **RECTAS** – Centre for Training in Aerospace Surveys
- **RCMRD** – Regional Centre for Mapping of Resources for Development
- **AOCRS** – African organization of Cartography and Remote Sensing

Others

- **AARSE** – African Association of Remote Sensing of the Environment
- **EIS-Africa**
- **ARMC** – African Resources Management Satellite
- **GMES-Africa**

…

2.3 DATA & CYBERSECURITY IN SPACE

AT THE NATIONAL LEVEL

Data

National laws on remote sensing

E.g. US, Canada, Germany, France (EU withdrew proposed Directive)

- Main **purpose**: national security
- Also: compliance with **UN principles**, promotion of private activity

Conditions:

- Prohibition, licensing
- Shutter control, priority access

Covers:

- **Data** – acquisition (direct reception by ground stations or market acquisition), processing, dissemination (market, Public Administration – GIS – export control issues)
- May also cover: **Systems** – launching, operation

National policies covering remote sensing

Licensing conditions:

- Policies of open access
- **Policies of restricted, reserved or controlled access**
- **Policies of exclusive / secret access**

(e.g., national security, classified information, data resolution, end-user, purpose of use)

Data granted:

- Raw
- Processed + value-added products

Rights:

- Use – purposes
- Processing and analysis – including combination (several data sources) (BDA – Big Data Analytics)

Data

Governance on remote sensing

State as a space actor – produces, acquirers and disseminates data

- Space agency
- Other entity: remote sensing centre, entities competent in cartography, meteorology and environment, public company, others

Space as a regulator – authorises and supervises space activities

- Space authority (independent regulator, ministry, public department)

Laws on data economy and privacy

Data economy

- Laws on freedom of information
- Laws on free flows of data in regional communities

No specific laws for satellite data

Data privacy

- Cross-sector laws on personal data
- Sector-specific laws on personal data (e.g., electronic communications, health)

No specific laws for the space sector

Cross-sector laws apply to the space sector (e.g., high resolution images that allow identification of personal data such as license plates)

Cybersecurity

Laws on space cybersecurity

Laws specifically applicable to the space sector

Cybersecurity is addressed in the space law or regulations

- E.g. UK: Space Industry Regulations (proposal) (which implement the Space Industry Act 2018

Laws on cybersecurity covering space

The space sector is covered in the general laws on cybersecurity or critical infrastructures

- E.g. Spain and France

Guidance on cybersecurity

Guidelines on cybersecurity for the space sector

E.g. UK – Cyber Security Toolkit by the UK Space Agency

E.g. US – Space Policy Directive-5

Cybersecurity addressed for national space programmes

E.g. EU – Flagship Programmes (Galileo/EGNOS, Copernicus, SST, GovSatCom)

03 RECOMMENDATIONS

Recommendations

Addressing Data issues in the Space sector is important because:

- Increases availability and quality of data for public and private purposes
- Decreases costs through alignment of all relevant public stakeholders
- Contributes to States' autonomy and preparedness
- Ensures compliance with UN principles (to the extent that a law on remote sensing is approved)
- Protects national security
- Attracts the private sector

1. Assess **current attributions and powers** in the acquisition of data for and within the Government / Public Administration
2. Assess the knowledge and **participation in international initiatives**
3. Define **aligned model or structure** for satellite data acquisition and use
4. Assess the **provision of data and value-added services**

(in both cases, assess collaboration initiatives with the private sector)

5. Assess the need for a **remote sensing law**, taking in consideration the State's capacities (human and material resources) and priorities
6. Create a **model for data sharing and free flow at the continental level** – Data Economy – and for a continental GIS (e.g., EU INSPIRE)

Recommendations

Addressing Cybersecurity issues in the Space sector is important because:

- Satellite systems are increasingly relevant for society, notably are essential for the maintenance of critical societal and/or economic activities and an incident would have significant disruptive effects
- Satellite systems are also vulnerable to cyber attacks
- Ensures compliance with UN principles
- Avoids or mitigates potential liability
- Attracts the private sector

1. Assess **current status of policies and laws on cybersecurity, critical infrastructures and cybercrime, including governance structures**
2. Assess participation in **international initiatives** on cybersecurity
3. Assess the need to issue **guidance, laws or regulations** on space cybersecurity
4. Assess the existence of **space programmes or systems requiring express compliance with cybersecurity provisions** or to be classified as critical infrastructure
5. Assess cybersecurity guidance and requirements for **continental space structures**
6. Ensure that cyber resilience and cyber incident response are always taken in consideration in the **private sector**

Contacts

Magda Cocco

Partner

✉ **mpc@vda.pt**

☎ T. 21 311 3487/519

VIEIRA DE ALMEIDA

www.vda.pt