
GOVERNMENT NOTICES • GOEWERMENTSKENNISGEWINGS

INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA

NO. 3172

17 March 2023



**NOTICE OF INTENTION TO CONDUCT AN INQUIRY IN TERMS OF SECTION 4B OF
THE INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA ACT, 2000
(ACT NO. 13 OF 2000) ON THE REVIEW OF THE REGULATIONS ON THE
CONVEYANCE OF MAIL, 2009.**

2023

INVITATION FOR WRITTEN REPRESENTATIONS

1. LEGAL BASIS FOR THE INQUIRY

- 1.1 The Independent Communications Authority of South Africa ("the Authority/ ICASA") is the regulator for the postal services sector as contemplated in section 3 (1A) of the Independent Communications Authority of South Africa Act, 2000 (Act No 13 of 2000) ('ICASA Act').
- 1.2 Section 8 (1)(a) of the PSA provides that the Authority must exercise regulatory functions in respect of reserved and unreserved postal services. Section 61 of the PSA provides that "*the Authority may make regulations regarding:*
- (a) *the carrying out of any international postal agreement or international postal arrangement entered into under this Act or by the Government;*
 - (b) *any matter which must or may be prescribed in terms of this Act;*
 - (c) *in general any matter which is necessary or expedient in order to achieve the objects of this Act; and*
 - (d) *the conveyance of postal articles, the general powers and duties of conveyers, legal possession or ownership of postal articles for purposes of contravention of this Act, mail fraud, theft and matters incidental thereto."*
- 1.3 The Authority is empowered by section 2 (bA) of the ICASA Act to regulate postal matters as contemplated in the PSA in the public interest.
- 1.4 Section 4B (1) of the ICASA Act in turn provides that: "*The Authority may conduct an inquiry into any matter with regard to:*
- (a) *the achievement of the objects of [the ICASA Act] or underlying statutes;*

- (b) *regulations and guidelines made in terms of [the ICASA Act] and the underlying statutes;*
- (c) *compliance by applicable persons with [the ICASA Act] and the underlying statutes;*
- (d) *compliance with the terms and conditions of any licence by the holder issued pursuant to the underlying statutes; and*
- (e) *the exercise and performance of the Authority's powers, functions and duties in terms of [the ICASA Act] or the underlying statutes."*

1.5 In terms of section 4B of the ICASA Act, ICASA hereby gives notice of its intention to conduct an inquiry on the Review of the Regulations on the Conveyance of Mail, 2009¹ ("Inquiry").

1.6 In conducting this Inquiry, the Authority is exercising its power in terms of section 4B (1) of the ICASA Act read with sections 8 (1)(a) and 61 of the PSA.

2. PURPOSE OF THE INQUIRY

2.1 The Regulations on the Conveyance of Mail, 2009 ("the Regulations") were published in 16 October 2009. The purpose of the Regulations is "to regulate:

- (a) *conveyance of mail and general powers and duties of the conveyors;*
- (b) *legal ownership and possession of mail; and*
- (c) *eradicate the exposure of mail to loss, damage and fraud."*

2.2 The postal services market has gone through changes since the Regulations were published. In the past ten (10) years, the sector has experienced a decline in letter mail volumes. In the same period there has been a growth of parcel delivery as result of proliferation of e-commerce services This has in turn led to data protection concerns from cybersecurity threats.²

¹ Government Gazette No32644 of 16 October 2009.

² Retrieved from <https://www.upu.int/.../Postal-economic-outlook-2021> on 15 November 2021.

- 2.3 The purpose of this Inquiry is to evaluate *the effectiveness of the current Regulations in dealing with the evolving consumer needs in changing market environment and then determine whether to amend or replace the Regulations.*

3. THE INQUIRY PROCESS

- 3.1 The Inquiry will be conducted in stages over a period of two (2) financial years. As the Inquiry unfolds, the Authority may introduce additional steps where necessary, but will keep stakeholders apprised of such developments.
- 3.2 To this end, the Authority publishes this Notice of Inquiry, together with the Discussion Document. The Authority hereby invites interested persons to submit their written representations to this Notice and the Discussion Document on the review of the Regulations on the Conveyance of Mail, 2009 ("Discussion Document").
- 3.3 A copy of this Notice of Inquiry and the Discussion Document will be made available on the Authority's website at <https://www.icasa.org.za/legislation-and-regulations/inquiries/regulations-on-the-conveyance-of-mail> and in the Authority's Library at 350 Witch-Hazel Road, Eco-park; Centurion between 09h00 and 16h00, Monday to Friday.
- 3.4 Written representations regarding this Notice of the Inquiry and the Discussion Document must be submitted to the Authority by no later than 16h00 on 26 May 2023 by email (in Microsoft Word and PDF) or hand delivery and marked specifically for attention:
- Mr. Sphiwe Hlongwane**
Delivery Address: 350 Witch-Hazel Road, Eco- Park; Centurion
Email: mailconveyance@icasa.org.za
- 3.5 This Discussion Document requires stakeholders to respond to a series of questions. **When responding to the questions, stakeholders are**

requested to explain their answers and support them with any relevant evidence and documentation where applicable.

- 3.6 Enquiries should be directed to Mr. Sipiwe Hlongwane at 012 568 3253 or Mrs. Esther Gopane at 012 568 3697; between 10h00 and 16h00, Monday to Friday.
- 3.7 In terms of section 4D of the ICASA Act, any person may request that any part of the written submission be treated as confidential. Requests for Confidentiality must be submitted in line with the Guidelines for Confidentiality Request in terms of section 4D of the ICASA Act published in Government Gazette No. 41839 of 17 August 2018.
- 3.8 Where an interested party has requested confidentiality on sections of its written submission, the written submission must be accompanied by one (1) non-confidential copy with sections that are redacted. The non-confidential version of the written submission will be published for public comment if the request for confidentiality is granted.
- 3.9 Requests for confidentiality will be considered within fourteen (14) working days of receiving the request. The Authority will communicate its decision to the respective Applicant.
- 3.10 Where the request for confidentiality is refused, the person who made the request will be allowed to withdraw such representations or portion(s) thereof.
- 3.11 Written representation(s) received by the Authority pursuant to this notice, will be made available for inspection by interested persons at the Authority's library and website. Library copies will be obtainable upon payment of the prescribed fee at ICASA Library at the following address: 350 Witch-Hazel Avenue, Eco Point Office Park, Eco Park, Centurion between 09h00 and 16h00, Monday to Friday.

- 3.12 Persons submitting written representations are further invited to indicate, as part of their submissions, whether they require an opportunity to make oral representations should the Authority decide to hold public hearings.
- 3.13 The Authority may hold public hearings on the issues raised in the context of this Inquiry if deemed necessary. The Authority will, notify stakeholders of the date, time and the venue in this regard.
- 3.14 The Inquiry will conclude with a Findings Document. The Authority will publish a Findings Document in the Government Gazette within 90 days from the date of conclusion of the Inquiry as prescribed in section 4C (6) of the ICASA Act.

4. Timelines

- 4.1 The Inquiry is envisaged to be conducted over a period of two (2) financial years 2022/23 and 2023/24. The Inquiry will culminate in a Findings Document that is envisaged to be published in March 2024.
- 4.2 The Inquiry may result in amendments to the Regulations or other appropriate interventions by the Authority in the financial year 2024/2025.
- 4.3 Timelines are subject to amendment by the Authority, but stakeholders will be duly notified of any amendments.



Dr Charles Lewis

Acting Chairperson

Date: 2023/ 03 / 06

DISCUSSION DOCUMENT
ON
THE REVIEW OF THE REGULATIONS ON
THE CONVEYANCE OF MAIL, 2009.

2023

TABLE OF CONTENTS

1.	Background.....	9
2.	Section A.....	11
2.1.	Introduction.....	11
2.2.	Methodology	12
3.	Section B.....	14
3.1.	Legal and Regulatory Context.....	14
3.1.2.	National Integrated ICT Policy White Paper and Postal Services Bill.....	14
3.1.3.	ICASA ACT No 13 of 2000	14
3.1.4.	Postal Services Act no 24 OF 1998 (PSA)	15
3.1.5.	International and Regional Instruments.....	16
4	Section C.....	18
4.1	Issues for Discussion.....	18
4.2	Purpose of the Regulations	18
4.3	Definitions	19
4.4	Scope	21
4.5	Legal Possession and Ownership of Mail.....	21
4.6	Postal Safety and Security	22
4.7	Dangerous and prohibited goods	31
4.8	Cybersecurity.....	38
4.9	Monitoring and Enforcement.....	47
4.10	Contraventions and Penalties.....	50
5	Section D	51
5.1	International Benchmarking.....	51
5.2	Malaysia	51
5.3	Tanzania	65
5.4	United States of America (USA).....	75
5.5	United Kingdom (UK).....	84
5.6	Zimbabwe.....	95
6	Lessons for Mail Conveyance Regulation in South Africa.....	104
7	Conclusion	110

1. BACKGROUND

- 1.1 The main business of traditional postal services is to deliver letters and small packages to businesses and the public. The growth and development of traditional mail business has been impacted by globalisation, market liberalisation, competition, and the advancement of new technologies. Despite the negative impact experienced over the last decade or so, the postal sector has evolved to play its role as an essential component of the global economy.³
- 1.2 Postal services continue to be a three-dimensional service, made up of physical, financial, and electronic postal services. The three (3) dimensions in postal services are categorised as the following:
- a. Physical services and related online letter business include basic letter services, basic parcel services, registered letters and parcels, addressing, retail outlets, collection points;
 - b. Digital and e-postal services include e-registered mail, hybrid mail, access to internet and e-mails, e-filing, fax mail, parcel and related online innovations such as parcel tracking and e-commerce; and
 - c. Financial services and associated ICT innovations includes sale cash on delivery, insured letters and parcels, issue and pay money orders, money transfers, postal orders, registered insured letters.
- 1.3 Postal services are defined to encompass:
- a) *"the service of conveying postal packets from one place to another by post,*
 - b) *the incidental services of receiving, collecting, sorting and delivering postal packets, and*

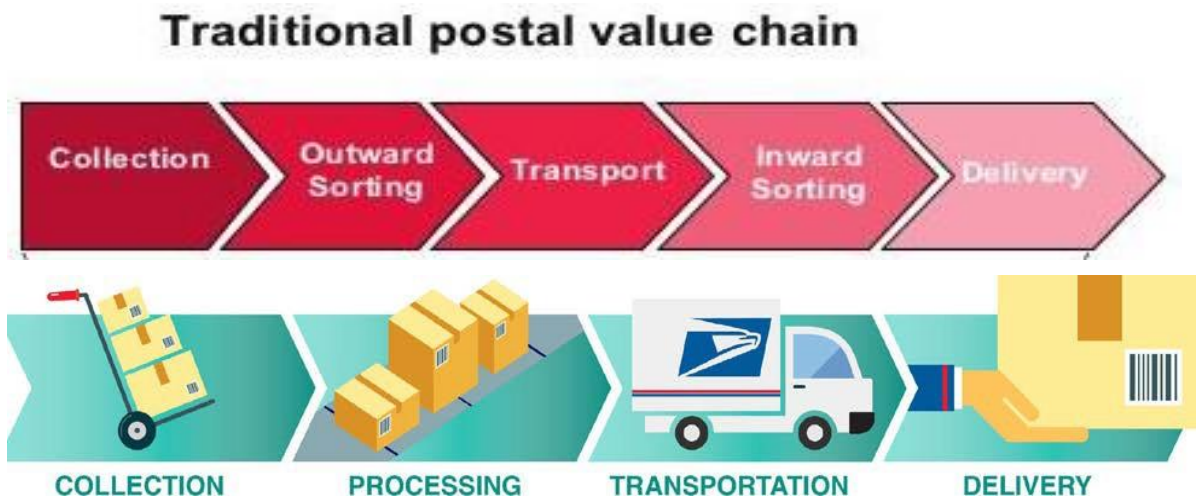
³ Retrieved from www.dohacongress.upu.int/strategy/ on 13 April 2021

c) any other service which relates to, and is provided in conjunction with, any service within paragraph (a) or (b).⁴

1.4 The United Nations International Standard Industrial Classification, Rev. 3.1 (ISIC), breaks down activities involved in postal services whether “national post” – reserved or “courier posts” – unreserved.⁵

1.5 These activities include the following:

*pickup, transport and delivery (domestic or international) of mail and parcels - collection of mail and parcels from public letterboxes or from post offices - distribution and delivery of mail and parcels - mailbox rental, poste restante etc. - mail sorting.*⁶ One or more modes of transport may be involved, and the activity may be carried out with either self-owned (private) transport or via public transport (in the context of private courier services). This class also includes: - home delivery services.⁷ The diagram below provides a presentation of the traditional postal value chain for letter and parcel mail:



Adopted from the United State Office of Inspector General (USOIG) publication.⁸

⁴ Retrieved from <https://www.legislation.gov.uk/ukpga/2011/5/section/27> on 23 April 2021

⁵ Retrieved from https://unstats.un.org/unsd/publication/SeriesM/seriesm_4rev3_1e.pdf on 13 April 2021

⁶ Retrieved from https://unstats.un.org/unsd/publication/SeriesM/seriesm_4rev3_1e.pdf on 13 April 2021

⁷ Retrieved from https://unstats.un.org/unsd/publication/SeriesM/seriesm_4rev3_1e.pdf on 13 April 2021

⁸ Retrieved from <https://www.uspsig.gov/document/issue-brief-rethinking-parcel-delivery-value-chain-recap-international-roundtable> on 23 April 2021

- 1.6 The goal is to deliver, to the right recipient, mail item contents in perfect conditions as collected from the sender. Even with dynamics brought by technological developments and market changes (e-commerce), the value chain activities remain the same.
- 1.7 In order to achieve this goal, postal services operations depend on both infrastructure and network. The postal infrastructure and network include, but are not limited to, buildings (retail offices, sorting centres), post boxes, collection boxes, and sorting and scanning machines, vehicles etc. This infrastructure network contributes to postal operators' success as a business and come with the security risk attached to them.⁹

Question 1: Considering the change in the market due to e-commerce, has the conveyance of mail value chain remained the same? Please elaborate.

2. SECTION A

2.1. INTRODUCTION

2.1.1 This Discussion Document is part of an Inquiry¹⁰ by ICASA into the Regulation on the Conveyance of Mail, 2009 ("the Regulations"). The Regulations are required by the Postal Services Act, 1998 (Act No 124 of 1998), ("PSA") in order to provide postal operators with requirements and processes to protect postal service resources, the process of conveyance and the handling of mail items under conveyance.

2.1.2 The Discussion Document is meant to facilitate participation and solicit stakeholder inputs in the process of evaluating whether the current Regulations cater to evolving consumer needs and whether they are in line with market and international trends and developments of the past decade.

⁹ Retrieved from https://about.usps.com/manuals/spp/html/spp7_066.htm on 24 April 2021

¹⁰ Section 4B of the ICASA Act, 2000 (Act No. 13 of 2000)

2.1.3 Security is a top priority: to limit exposure of mail items to risks of loss, theft, fraud, damage and tampering. Security and safety entail wide-ranging tasks that take into consideration the variety of mail items that can be conveyed over the postal network, and different processes and human resources required to handle different types of mail items.¹¹

2.1.4 The PSA enforces sanctions against any person who forges, alters, imitates etc. postal infrastructure and endangers mail items in possession of the postal operator or the conveyance process.

2.1.5 This Inquiry will allow the Authority to review the required measures and processes in place to ensure integrity of the postal services.

2.1.6 The inquiry is envisaged to be conducted over a period of two (2) financial years, viz 2022/23 and 2023/24.

2.1.7 The inquiry will culminate in a Findings Document that is envisaged to be published in March 2024.

2.2. METHODOLOGY

2.2.1 The methodology applied in formulating the Discussion Document includes desktop research, policy and legislative analysis.

2.2.2 The documents analysed include the National Integrated ICT Policy White Paper "White Paper",¹² the PSA and international instruments (i.e. conventions, guidelines, treaties, etc.) that have a bearing in the regulation of postal service, and the Conveyance of Mail Regulations, 2009.

¹¹ Retrieved from https://about.usps.com/manuals/spp/html/spp7_066.htm on 24 April 2021

¹² Retrieved from https://www.gov.za/sites/default/files/gcis_document/201610/40325gon1212.pdf on 22 July 2022

2.2.3 The process commenced with desktop research on issues related to conveyance of mail including international benchmarking. The countries selected for international benchmarking provide valuable lessons for the South African context. The main considerations for benchmark selection include: the level of development of the postal regulatory framework; availability and accessibility of information; and the evolution of postal services.

3. SECTION B

3.1. LEGAL AND REGULATORY CONTEXT

3.1.1 This section of the Discussion Document provides the domestic legislative context to postal services, specifically with respect to provisions of empowering legislation which afford the Authority the necessary power to conduct an inquiry in terms of section 4B of the ICASA Act. This section also highlights international instruments that have a bearing in the regulation of mail conveyance.

3.1.2. NATIONAL INTEGRATED ICT POLICY WHITE PAPER AND POSTAL SERVICES BILL

3.1.2.1 Chapter 11 of the White Paper deals with Postal Policy. For purposes of this Discussion Document, it suffices to state that the White Paper makes several interventions, which among others have a bearing in the future regulation of the postal sector. Although the Postal Services Amendment Bill (2017)¹³ ("the Bill") is yet to be finalised, it does to a certain extent incorporate the prescripts of the White Paper.

3.1.3. ICASA ACT NO 13 OF 2000

3.1.3.1 The Authority is empowered by section 2 (bA) of the ICASA Act to regulate postal matters, as contemplated in the PSA, in the public interest.

3.1.3.2 In terms of section 4B of the ICASA Act, the Authority is empowered to conduct an inquiry into any matter regarding:

"(a) the achievement of the objects of the ICASA Act or underlying statutes;

¹³ Postal Services Bill, Government Gazette No. 41246, of 10 November 2017

(b) regulations and guidelines made in terms of the ICASA Act and the underlying statutes;

(c) compliance by applicable persons with the ICASA Act and the underlying statutes;

(d) compliance with the terms and conditions of any licence by the holder issued pursuant to the underlying statutes; and

(e) the exercise and performance of the Authority's powers, functions and duties in terms of this Act or the underlying statutes."

3.1.3.3 The ICASA Act defines "underlying statutes", which includes the Postal Services Act.

3.1.4. POSTAL SERVICES ACT NO 24 OF 1998 (PSA)

3.1.4.1 The definition of postal services as set out in the PSA means "a reserved postal service or an unreserved postal service as contemplated in Schedule 1 and Schedule 2 respectively".

3.1.4.2 The Authority is empowered by section 2 of the PSA, which provides for the regulation and control of postal services in the public interest and for that purpose to:

"(m) promote the effective maintenance of an efficient system of collecting, sorting, and delivering mail nationwide, in a manner responsive to the needs of all categories of mail users;

(d) encourage investment and innovation in the postal industry;

(e) promote the development of postal services that are responsive to the needs of users and consumers;

(j) protect the interests of postal users and consumers;

(p) ensure compliance with international commitments."

3.1.4.3 Section 61 (d) of the PSA empowers the Authority to make regulations regarding:

"(d) The conveyance of postal articles, the general powers and duties of the conveyers, legal possession or ownership of postal articles for purposes of contravention of this Act, mail fraud, theft and matters incidental thereto."

3.1.5. INTERNATIONAL AND REGIONAL INSTRUMENTS

3.1.5.1 The Authority's work in regulation of postal services is also guided by instruments that are developed by the international and regional associations wherein South Africa is a member.

3.1.5.2 These associations include the Universal Postal Union ("UPU"), Pan African Postal union ("PAPU") and Communications Regulators Association of Southern Africa ("CRASA").

3.1.5.3 The UPU is a United Nations body that provides general postal policies and model regulations for member countries. The UPU continuously engages and collaborates with international organisations such as the World Customs Organisation ("WCO"), the International Air Transport Association ("IATA") etc. to draw guidelines for security and safety of conveying mail. The UPU provides general guidelines on issues and encourages countries to apply the guidelines best suited for their environment.

3.1.5.4 PAPU is a specialized institution of the African Union. Its main objective is to coordinate all activities aimed at developing postal services on the African continent.

3.1.5.5 CRASA is a consultative body of regulators dealing in the telecommunications, broadcasting and postal sectors for the Southern African region.

3.1.5.6 The discussion document will draw reference from the following guidelines developed by the above-mentioned associations:

- a. The UPU Postal security –UPU General Security Measures S58 and S59 documents.¹⁴
- b. IATA–UPU Mail Safety Guidelines: Recommendations to Designated Postal Operators¹⁵
- c. WCO–UPU Postal Customs Guide, (2018).¹⁶
- d. CRASA Postal Security & Integrity Guidelines; (2016) for the designated postal operators (DPOs) in SADC.¹⁷

3.1.5.7 CRASA has developed guidelines on postal security and integrity: Postal Security & Integrity Guidelines; (2016) for the designated postal operators (DPOs) in SADC, as they are an official port of entry for mail coming from foreign countries.¹⁸

3.1.5.8 CRASA Postal Security & Integrity Guidelines is offered as a reference source to guide Member States in the establishment of a policy and regulatory framework that promotes postal security and integrity in the SADC Region. It is applicable to all areas of postal services (reserved and unreserved). This guideline draws into consideration international best practices and principles outlined by the UPU.¹⁹

¹⁴ Retrieved from; <https://www.upu.int/en/Postal-Solutions/Programmes-Services/Postal-Supply-Chain/Security#postal-security-standards> on 18 July 2022

¹⁵ Retrieved from https://www.upu.int/UPU/media/upu/files/postalSolutions/programmesAndServices/postalSupplyChain/Security/Mail%20Safety%20Guidelines/En_cep_c_1_gsp-2_d005b_ad00_an01_p00_r00.pdf on 18 July 2022

¹⁶ Retrieved from <http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/wco-upu-postal-customs-guide> on 18 July 2022

¹⁷ Retrieved from <https://www.crasa.org/crasa-publication/cat/35/postal-regulatory-guidelines/> on 15 April 2021

¹⁸ Retrieved from <https://www.crasa.org/crasa-publication/cat/35/postal-regulatory-guidelines/> on 15 April 2021

¹⁹ Retrieved from <https://www.crasa.org/crasa-publication/cat/35/postal-regulatory-guidelines/> on 15 April 2021

4 SECTION C:

4.1 ISSUES FOR DISCUSSION

4.1.1 This section focuses on issues covered in the current regulations which are also provided for by international conventions. Further it includes other issues which currently impact on the safety and security of mail or which form part of mail conveyance value chain. These issues include the following:

- a. Purpose of the Regulations;
- b. Definitions;
- c. Scope;
- d. Legal possession and ownership of mail;
- e. Postal safety and security;
- f. Dangerous and prohibited goods; and
- g. Contraventions and penalties.

4.1.2 Another issue to be considered, which is currently not included in the Regulations, is cybersecurity.

4.2 PURPOSE OF THE REGULATIONS

4.2.1 The Authority published the Regulations on 16 October 2009. The purpose of the Regulations is to regulate:

- (a) conveyance of mail and general powers and duties of the conveyors;
- (b) the legal ownership and possession of mail; and
- (c) eradicate the exposure of mail to loss, damage and fraud.

Question 2: Do you think the Regulations fulfil the following purposes as intended?

Purpose	Yes/No	Elaborate
Regulating the conveyance of mail?		
Provisioning for the general powers and duties of conveyors?		
Regulating possession and ownership of mail?		
Eradicating exposure of mail to risk of loss, theft, fraud, damage, delay, or tampering?		
Question 3: Do the Regulations protect the interests of postal consumers?		

4.3 DEFINITIONS

4.3.1 This section will look into several definitions that are critical to the Regulations.

4.3.2 The three commonly used terms in the postal sector relating to mail conveyance are the following: "mail"; "conveyance" and "post". Currently in the legislation and the regulation there is no definition of mail conveyance as a single term.

4.3.3 The PSA defines "mail" as *"every article collected for conveyance by post and includes loose and individual articles and every mail bag, vessel or conveyance of any kind by which postal articles are carried, whether or not it contains any such articles and every person conveying or delivering mail or postal articles"*.

- 4.3.4 The PSA does not define “conveyor”. However, the Regulations define a conveyor as “a person or a licensee whose business is to carry, transfer or deliver mail from the sender to the intended destination”²⁰.
- 4.3.5 The term “post” is also not defined in the PSA and the Regulations. From the research conducted, “post” may be defined as “written communication and/or electronic mail services, parcel services, logistics services, financial transaction services, and postal agency services for public interests.”²¹
- 4.3.6 Similar to the PSA, the UPU does not define mail conveyance as one single term. The UPU glossary standard defines a “mail item” as an “indivisible mailable entity in respect of which a mail service contractor accepts an obligation to provide postal services... Items should be handled and delivered as an integrated unit and not split into components within the postal system.” These *may include, letter mail (items), parcel post (items), registered mail (items)*. The term conveyor is not defined in the UPU glossary of terms.

Question 4: Should the Regulations provide a definition for “post”?

Question 5: Should the regulations provide a definition for “mail conveyance”?

Question 6: Do you think the definition of “conveyor” in the Regulations includes all operators involved in the process of mail conveyance?

Question 7: Do you think there are additional terms that the Authority should define in the regulations?

²⁰ Government Gazette No 32644 of 16 October 2009.

²¹ Retrieved from <https://jdih.kominfo.go.id/storage/files/1574058949- JDIH 3 Law No 38 of 2009 on Post.pdf> on 02August 2022

4.4 SCOPE

4.4.1 The Regulations apply to all conveyors of mail as defined in the Regulations and any licensee or postal operator falling under the ambit of Schedule 1 and 2 of the PSA and whose business includes to carry, transfer or deliver mail from the sender to the intended destination is subject to the Regulations.

4.5 LEGAL POSSESSION AND OWNERSHIP OF MAIL

4.5.1 Regulation 5 of the Regulations states the following:

"(5.1) the conveyor is deemed to possess the mail from the moment that mail is handed to the conveyor or his agent".

(5.2) possession of mail passes to the addressee, upon delivery of mail.

(5.3) the conveyor is liable for damage, loss, and theft of mail from the point of receipt of the goods until the delivery of the goods is completed."

4.5.2 Section 33 of the PSA provides the following four (4) positions, which defines when postal articles can be regarded as being in the course of transmission or have been posted or delivered:

"(a) a postal article shall be deemed to be in the course of transmission by post from the time of its being delivered to a post office to the time of its being delivered to the person to whom it is addressed.

(b) the placing of a postal article of any description in a pillar box or other receptacle provided for this purpose by or with the approval of the postal company, or the delivery of a postal article to a postman or other person authorised to receive postal articles of that description for the post, must be regarded as being delivery to a post office.

(c) the delivery of a postal article at the house or office of the person to whom the article is addressed, or to his or her servant or agent or other person considered to be authorised to receive the article according to the usual manner of delivering that person's postal articles, or at the address specified on such article, must be regarded as being delivery to the person to whom the article is addressed.

(d) delivery into a private box or private bag must be regarded as being in all respects equivalent to personal delivery to the addressee.”²²

4.5.3 In terms of ownership of mail, the UPU conventional manual article 5 provides that “postal items shall remain the property of the sender until it is delivered to the rightful owner, except when the item has been seized in pursuance of the national legislation of the country of origin or destination”.²³

4.5.4 The terms “ownership” and “legal possession” of mail assist conveyors with issues of claims for loss and damage. Based on the aforementioned, the current Regulations are in line with the UPU provision for ownership and legal possession of mail.

Question 8: Do the regulations clearly indicate the difference between “ownership” and “legal possession”?

4.6 POSTAL SAFETY AND SECURITY

4.6.1 The safety and security of the postal sector as part of the global supply chain is critical to supporting worldwide commerce and communication. Hintsa et al

²² Postal Services Act no 124 of 1998. Government Gazette No.40584 of 30 January 2017

²³ Retrieved from

<https://www.upu.int/UPU/media/upu/files/UPU/aboutUpu/acts/manualsInThreeVolumes/actInThreeVolumesManualOfConventionMaj1En.pdf> on 15 April 2021

point to the open nature of the postal system, as well as large volumes of customers and shipments, as top reasons driving security vulnerabilities in the system.²⁴

4.6.2 The physical infrastructure and mail items are not the only parts in the postal value chain that needs protection. The safety of postal sector employees and customers must also be included and treated as critical to the entire postal supply chain.²⁵ The security threat can be internal as well as external.

4.6.3 The Regulations obligate conveyors to put in place measures against loss, theft, fraud, damage, and tampering, and to maintain strict access control to areas where mail is kept. Measures may include installation of surveillance equipment and alarm systems that limit access to authorised personnel. Conveyors must also oversee the whole process of mail conveyance, from receiving mail to screening mail for possible prohibited and dangerous goods, while ensuring that all risk assessments are conducted to prevent and monitor loss, theft, damage, or tampering of mail.

4.6.4 Article 8 of the UPU Convention Manual on postal security provides that “member countries shall adopt and implement a proactive security strategy at all levels of postal operations to maintain and enhance the confidence of the general public in the postal services, in the interests of all officials involved.”²⁶

4.6.5 Furthermore, the general security measures recommended by the UPU aim to enhance the security of all operations within the postal sector by defining a minimum physical and process security requirement applicable to critical facilities within the postal network.

²⁴ Hintsä, J, Hameri, A-P, Tsikolenko, V & Männistö, T (2010) ‘Crime and security in postal supply chains’, retrieved from https://www.researchgate.net/publication/282664579_Crime_and_security_in_postal_supply_chains on 07 December 2021.

²⁵ Retrieved from <https://www.upu.int/en/Postal-Solutions/Programmes-Services/Postal-Supply-Chain/Security> on 13 May 2021

²⁶ Retrieved from <https://www.upu.int/UPU/media/upu/files/UPU/aboutUpu/acts/manualsInThreeVolumes/actInThreeVolumesManualOfConventionMaj1En.pdf> on 15 May 2021

4.6.6 The general measures take into consideration security standards, the 'UPU General Security Measures S58', the 'UPU Postal security – Office of Exchange and International Airmail Security S59'. Together these recommendations deal with physical and personnel security, and the actual screening of the mail respectively.²⁷ These standards are recognised by the WCO as being equivalent to their safe framework of standards, which intends to "act as a deterrent to international terrorism, secure revenue collections and promote trade facilitation worldwide."²⁸

4.6.7 **Physical security measures and processes for mail safety**

4.6.7.1 Postal physical infrastructure includes all physical machines, buildings (sorting and distribution centres), post boxes, collection boxes, mailbags, vehicles, etc., that contribute to the processing and completion of the postal value chain activities.

4.6.7.2 The Regulations do not have a provision pertaining to the damage of postal physical infrastructure. However, the Authority does receive complaints relating to damaged physical postal infrastructure, including requests for maintenance and upkeep of postal infrastructures.

4.6.7.3 According to the UPU, general physical security requirements for critical postal facilities should include, as appropriate, a combination of security measures such as:

- a. perimeter barriers like fencing and walls installed to deny access of non-authorised individuals or vehicles onto restricted areas of the critical facility;

²⁷ Retrieved from <https://www.upu.int/UPU/media/upu/files/postalSolutions/programmesAndServices/postalSupplyChain/Security/s58En.pdf> on 15 May 2021

²⁸ Retrieved from http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/frameworks-of-standards/safe_package.aspx on 15 May 2021

- b. adequate lighting to illuminate parking, entrance, pedestrian areas etc. sufficiently to identify individuals or vehicles within close proximity;
- c. locking mechanisms and key control, uniformed or identifiable security guards/personnel, CCTV, and alarm/intrusion detection systems.²⁹

4.6.7.4 With regards to transportation for conveyance of mail, the UPU General Security Measures S58 recommends that “the DPO [should] document processes and procedures for security of the mail by all modes (air, road, sea, and rail) of transportation and comply with national legislation and transportation standards.”³⁰

4.6.7.5 Moreover, in order to safeguard transportation of mail, the following standard is recommended:

- a. *vehicles must be designed from resilient materials and possess features such as a solid-top, hard sides or reinforced soft-sides and locked cargo doors. Inspection of vehicles must be conducted before loading and report if there are any signs of tampering.*
- b. *When loaded with mail, in transit, or left unattended on the premises, all access points to the mail shall be secured (locked).*
- c. *possibly, all vehicles must be clearly marked or identifiable as an authorised postal vehicle or postal contracted vehicle.*
- d. *possibly all postal vehicle drivers must wear a designated postal uniform and/or possess and clearly display a valid form of postal or contractor identification.*
- e. *Vehicle cabin and key ignitions must be secured from unauthorised access.*
- f. *a key accountability process must be maintained.*
- g. *vehicles, conveyance or containers shall be properly emptied.*

²⁹ Postal security – General security measures – S58, retrieved from <https://www.upu.int/UPU/media/upu/files/postalSolutions/programmesAndServices/postalSupplyChain/Security/securityStandards/s58-4En.pdf> on 18 January 2022

³⁰ Postal security – General security measures – S58, retrieved from <https://www.upu.int/UPU/media/upu/files/postalSolutions/programmesAndServices/postalSupplyChain/Security/securityStandards/s58-4En.pdf> on 18 January 2022

- h. routes, schedules and planned stops shall be assessed for risk and, if necessary, an additional security measure shall be initiated to mitigate the risk.*
- i. an annual compliance audit shall be conducted by personnel independent of the critical facility management team.³¹*

Question 9: Do you think the Regulations make enough provision for the safety of mail items? Please elaborate under the following safety aspects:

	YES/NO	Elaborate
Physical Infrastructure		
Personnel Security		
Mail Processing Operations		

Question 10: Do you think the Regulations take into consideration the UPU's general security measures? If your answer is No, in your view which of the UPU security measures should the Authority consider?

Question 11: Do you think the safety of mail, either in storage or in transit, is sufficiently addressed by the Regulations?

³¹ Postal security – General security measures – S58, retrieved from <https://www.upu.int/UPU/media/upu/files/postalSolutions/programmesAndServices/postalSupplyChain/Security/securityStandards/s58-4En.pdf> on 18 January 2022

4.6.8 Protection against loss or damaged mail

- 4.6.8.1 Loss of mail can be attributed to several risk factors, including internal neglect, external hijackings, or incorrect addressing provided by the sender. For instance, with the growth of cross border e-commerce, postal operators convey parcels, some of which may be of high value and attractive appearance, leading to theft by postal sector employees or external thieves.
- 4.6.8.2 There have been reports of hijacking and attacks on courier vehicles. This may be due to criminals being aware that couriers convey high-value commodities, many of which are attractive and can be sold very easily.³²
- 4.6.8.3 Negligence with respect to safety and security measures can also compromise the postal operator's reputation, which in turn affects the mail business. A survey by MyBroadband indicates that South Africans have lost faith in the SA Post Office. Many tell stories of lost packages, late mail or treasured items that have seemingly vanished.³³
- 4.6.8.4 Another form of negligence that can occur and lead to damage and loss of mail may come about during processing of mail from collection to delivery since mail passes through different systems and is handled by different personnel.
- 4.6.8.5 Unfortunately, there are some reports of postal service employees who have stolen mail items, while others, due to lack of training in handling mail items, may jeopardise the safety of mail items and damage them. The SAPO 2020 Annual Report makes some mention of loss of revenue due to loss,

³² Labuschagne, H. Shoot first, steal later – South African courier hijackings worse than ever, retrieved from <https://mybroadband.co.za/news/motoring/387630-shoot-first-steal-later-south-african-courier-hijackings-worse-than-ever.html> on 15 May 2021

³³ It's official – Online shoppers do not trust the SA Post Office, retrieved from <https://mybroadband.co.za/news/it-services/300424-its-official-online-shoppers-do-not-trust-the-sa-post-office.html> on 12 November 2021

theft, damage to the post office infrastructure, and mail item claims, although it does not provide clear statistics of cases in record.³⁴

- 4.6.8.6 The Authority receives more complaints relating to parcels than to letters/mail. The complaints range from lost or stolen parcels, damaged parcels, delay in delivery of parcels (unreasonable time frame), and undue claim processes on stolen, lost, and damaged parcels. Consumers have an option of insuring mail items. However, the challenge with the current insurance system is that the insurance threshold does not fully cover the value of the conveyed mail item.
- 4.6.8.7 Furthermore, consumers have lodged complaints regarding delays in delivery of mail, and lack of notification about such delay to the sender or the addressee. In some cases, conveyors will only make an announcement after the Authority has raised a concern, or after receiving too many complaints from customers waiting for mail/parcels.
- 4.6.8.8 When dealing with the delay of mail, the conveyor has to notify the sender within a reasonable period of its inability to deliver the mail on time, and such notification should cover at least the channels of SMS, email, telephone or radio announcement.
- 4.6.8.9 UPU General Security Measures S58 recommends that personnel security and training shall be deployed in order to reduce and minimise security risks to the business, its customers, and employees.
- 4.6.8.10 In this instance, the UPU General security measures S58 recommends the following for personnel security:

³⁴ South African Post Office SOC LTD Annual Report 2020, retrieved from <https://www.postoffice.co.za/about/ar2020.pdf> on 15 April 2021

- a. *training shall be deployed in order to reduce and minimise security risks to the business, its customers and employees.*
- b. *personnel selection must be documented for every employee working within the facilities and/or handling mail at external locations.*
- c. *hiring process must be in consistent with the national legislation.*
- d. *background check must be conducted for all employees.*
- e. *process to communicate employee performance and misconduct must be maintained.*
- f. *termination shall be documented and include timely return of identification documents, access control devices, keys, uniforms and other sensitive information.*
- g. *a record must be maintained to ensure that there is no re-hiring of employees whose termination was due to misconduct.*
- h. *if mail handling is conducted by a contractor, the contractor shall follow the same process of employment, termination, and misconduct. The contractor must inform the DPO of any personnel findings or decisions which could pose potential security risks to the operation.*
- i. *security awareness training must be documented and maintained for all employees and contractors.*

4.6.8.11 Postal operators are also guided by the UPU and CRASA guidelines to put in place personnel screening and training to handle and process mail items in order to minimise incidents of neglect and damage or loss and theft.

4.6.8.12 CRASA guidelines on postal safety and security recommends the following actions in line with the UPU manuals:

- a. periodic risk assessment of physical location, and its accessibility to employees and the public, to ensure safe mail handling standards;
- b. centralisation of mail operations;
- c. designing a physical layout for mail centres which minimises operations risk;

- d. establish sound security protocols (rules and procedures) for each of their retail and mail processing facilities;
- e. maintain physical security/safe work environment that promotes security and integrity of mail at all times, while protecting employees and assets including physical security personnel;
- f. conduct pre-employment screening of all potential employees; and
- g. regular training and education provision for different areas of mail handling personnel and create a culture of security awareness.³⁵

4.6.8.13 In terms of wrongly addressed mail, the post office has a return letter office (RLO) where these items are kept for a certain period before they are destroyed or auctioned if not claimed by anyone.

Question 12: Do you think insurance should be compulsory for all conveyed items? If yes, who should be responsible for taking out insurance for mail items?

Question 13: Do you have any further suggestions on remedies that can be put in place to ensure the safe conveyance of mail items?

Question 14: Do you think there should be a rebate payable to the sender where there has been a delay in the delivery of an item/article without a notification for such delay?

³⁵ CRASA. Guidelines on postal security, retrieved from <https://www.crasa.org/crasa-publication/cat/35/postal-regulatory-guidelines/> on 15 April 2021

4.7 DANGEROUS AND PROHIBITED GOODS

- 4.7.1 Postal operations can be targeted and used to convey dangerous/harmful and illegal goods by terrorists and others wishing to cause harm or disruption to recipients e.g., bomb, anthrax, etc.
- 4.7.2 The Regulations have placed an obligation on the conveyor to publish a list of dangerous goods that must not be delivered through mail. Regulation 4.7 also requires the conveyor to ensure that suspicious mail is detected and disposed. From a consumer perspective, there has not been complaints about conveyance of dangerous goods, however, the Authority has received reports from operators about discovering dangerous goods in the postal system.
- 4.7.3 Furthermore, the Regulations also placed an obligation on the conveyor to publish a list of prohibited goods that must not be delivered through mail. However, the growth of e-commerce has seen packages/parcels that were initially regarded as Prohibited Goods under the Schedule B of the Regulations on Conveyance of Mail being conveyed through the mail.
- 4.7.4 The Authority has received complaints from consumers about lost, stolen, or damaged parcels that carry items such as uninsured handsets, uninsured jewellery, and cannabis.
- 4.7.5 The UPU provides the following interventions for handling dangerous goods. Firstly, the insertion of dangerous goods as described in the convention manual and Regulations shall be prohibited in all categories of items. Article 19 of the UPU convention manual lists the following prohibited items:³⁶
- a. "Narcotics and psychotropic substances, as defined by the International Narcotics Control Board (INCB), or other illicit drugs which are prohibited in the country of destination.

³⁶ UPU Convention Manual, retrieved from <https://www.upu.int/UPU/media/upu/files/UPU/aboutUpu/acts/manualsInThreeVolumes/actInThreeVolumesManualOfConventionMaj1En.pdf> on 15 May 2021

- b. obscene or immoral articles; counterfeit and pirated articles; other articles the importation or circulation of which is prohibited in the country of destination.
 - c. articles which, by their nature or their packing, may expose officials or the general public to danger, or soil or damage other items, postal equipment, or third-party property.
 - d. documents having the character of current and personal correspondence exchanged between persons other than the sender and the addressee or persons living with them.”³⁷
- 4.7.6 Further, the manual provides that “all member countries or their designated operators shall have the option of extending the prohibitions contained in this article, which may be applied immediately upon their inclusion in the relevant compendium.”³⁸
- 4.7.7 The UPU places the responsibility to inform customers about the prohibited items with the postal operators and encourages them to publish this list on their websites and their postal operation sites.
- 4.7.8 Secondly, the convention manual provides for exceptions of dangerous goods that can be allowed to be moved within postal networks. Listed dangerous goods under article 19-001 of the UPU Manual may exceptionally be admitted between member countries that have declared their willingness to admit them either reciprocally or in one direction.
- 4.7.9 The exceptions are listed under the following three (3) classes:
- a. Class 7 – Radioactive materials
 - b. Class 6.2 - Infectious substances

³⁷ UPU Convention Manual, retrieved from <https://www.upu.int/UPU/media/upu/files/UPU/aboutUpu/acts/manualsInThreeVolumes/actInThreeVolumesManualOfConventionMaj1En.pdf> on 5 August 2021

³⁸ UPU Convention Manual, retrieved from <https://www.upu.int/UPU/media/upu/files/UPU/aboutUpu/acts/manualsInThreeVolumes/actInThreeVolumesManualOfConventionMaj1En.pdf> on 5 August 2021

- c. Class 9 – Lithium metal cells and lithium-ion batteries contained in equipment³⁹

4.7.10 If member countries choose to ship dangerous goods, it is required that they know and follow various stipulations in the regulations (national and international), including details on the types of packaging, documentation, and labelling required and variations depending on the mode of transport to be used. They must also ensure proper training for everyone handling dangerous goods.⁴⁰ Examples of dangerous goods and how they should be conveyed through mail will be listed below:

4.7.11 Radioactive materials admitted in letter-post items and parcels

- a. shall be subject to the tariff for priority items or the tariff for letters and registration.;
- b. shall be forwarded by the quickest route, normally by air, subject to payment of the corresponding surcharges, and
- c. may be posted only by duly authorised senders.

4.7.12 Infectious substances are listed in Category A (UN 2814) and Category B (UN 2900)

- a. Category A are those materials that should one be exposed to, they are capable of causing permanent disability, life threatening or fatal disease in otherwise healthy humans. Examples include Hepatitis B virus (cultures only); Herpes B virus (cultures only); Human immunodeficiency virus (cultures only) etc.

³⁹ IATA-UPU Mail Safety Guidelines Recommendations to DPOs, retrieved from <https://www.iata.org/contentassets/15ee3a255dc447b886d9a7e91fa65dbe/mail-safety-requirements.pdf> on 15 May 2021

⁴⁰UPU Convention Manual, retrieved from <https://www.upu.int/UPU/media/upu/files/UPU/aboutUpu/acts/manualsInThreeVolumes/actInThreeVolumesManualOfConventionMaj1En.pdf> on 5 August 2021

- b. Category B are substances which are known or are reasonably expected to contain pathogens (including bacteria, viruses, parasites, fungi) and affect animals.

4.7.13 They are accepted in letter-post items and postal parcels; however, under article 19, resolution CA 6/2006 prohibits the carriage of Category A infectious substances in international mail. The following conditions should be met for carriage in postal systems:

- a. exchange may be by mail only between officially recognised senders, as determined by their competent authority.
- b. must be handled, packed and labelled in accordance with the provisions listed in the Regulations (the Transport of Dangerous Goods (Model Regulations ST/ SG/AC10/1) as discussed below.
 - i. *Subjected to the national and international legislation in force and the current edition of the United Nations Recommendations on the Transport of Dangerous Goods, as promulgated by the ICAO.*⁴¹
 - ii. *shall be subjected to the tariff for priority items or the tariff for registered letters. An additional charge for the handling of these items shall be allowed.*
 - iii. *shall be restricted to member countries that have declared their willingness to admit such items, whether reciprocally or in one direction only.*
 - iv. *shall be forwarded by the quickest route, normally by air, subject to the payment of the corresponding air surcharges, and shall be given priority in delivery.*
- c. Packaging of infectious substances must meet the following criteria as regulated⁴²:
 - i. *Must be appropriately marked with the words in English or French "Exempt human specimen"/" Echantillon humain exempté" or "Exempt animal specimen"/" Echantillon animal exempté",*

⁴¹ Retrieved from <https://www.icao.int/safety/DangerousGoods/htmls/StateVariation.en.html> on 15 January 2022

⁴² UPU convention Manual, retrieved from <actInThreeVolumesManualOfConventionMaj1En.pdf> (upu.int) on 15 January 2022

- ii. Packaging must contain a leak-proof primary receptacle(s);*
 - iii. a leak-proof secondary packaging; and*
 - iv. an outer packaging of adequate strength for its capacity, mass, and intended use, and with at least one surface having minimum dimensions of 100 mm × 100 mm; Volume I – 73*
 - v. For liquids, absorbent material in sufficient quantity to absorb the entire contents must be placed between the primary receptacle(s) and the secondary packaging so that, during transport, any release or leak of a liquid substance will not reach the outer packaging and will not compromise the integrity of the cushioning material,*
 - vi. Fragile primary receptacles must be either individually wrapped or separated to prevent contact between them when they are multiple and placed in a single secondary packaging.*
- d. Lithium cells are allowed under the following conditions:*
- i. it must be a maximum of four (4) or two (2) batteries installed into an equipment.*
 - ii. lithium content cannot be more than 1g for a lithium-ion cell and the watt-hour (Wh) rating shall not be more than 20 Wh.*
 - iii. lithium metal or lithium alloy battery, must not contain more than 2g*
 - iv. lithium-ion battery, the Wh rating shall not be more than 100 Wh; Lithium-ion batteries subject to this provision shall be marked with the Watt-hour rating on the outside case.*
 - v. When packaging the equipment installed with Cells and batteries it must be made sure that the package is protected from damage and short circuit, and the equipment shall be equipped with an effective means of preventing accidental activation.*
 - vi. when lithium batteries are installed in equipment, they shall be packed in strong outer packaging constructed of suitable material of adequate strength and design in relation to the packaging's capacity and its intended use unless the batteries are afforded equivalent protection by the equipment in which they are contained.*

vii. *Each cell or battery shall be of the type proved to meet the requirements of each test⁴³ in United Nations Manual of Tests and Criteria⁴⁴, Part III (Relating to aerosols, desensitised explosives (relating to transport only), subsection 38.3 (8 module test which are: Altitude Simulation (Primary and Secondary Cells and Batteries); Thermal Test (Primary and Secondary Cells and Batteries); Vibration (Primary and Secondary Cells and Batteries); Shock (Primary and Secondary Cells and Batteries); External Short Circuit (Primary and Secondary Cells and Batteries); Impact (Primary and Secondary Cells); Overcharge (Secondary Batteries); Forced Discharge (Primary and Secondary Cells)).*

4.7.14 The UPU together with the International Air Transport Association (IATA), developed an (IATA-UPU) mail safety guidelines for any mail transit in air transport.⁴⁵ The mail safety guideline takes into consideration UPU Postal security – Office of exchange and international airmail security S59, standard for mail screening. IATA is the trade association for the world’s airlines, supporting various areas of aviation activity and help formulate industry policy on critical aviation issues.

4.7.15 The guidelines provide four key aspects recommended for DPOs and these include the following;

- a. *training of frontline staff to ask questions and raise awareness on the impact of dangerous goods being inserted in the mail;*
- b. *training for DPOs to ensure safe airmail handling. From preparation, unit load device safety to acceptance of mail;*
- c. *harmonisation and standardisation of the oversight programs from the Regulators – this requires participation of all stakeholders: National Aviation Authority (NAA), DPOs, UPU and regulators; and*

⁴³ test methods and procedures to be used for classification of dangerous goods according to the provisions of the "United Nations Recommendations on the Transport of Dangerous Goods, Model Regulations.

⁴⁴ Retrieved from <https://unece.org/about-manual-tests-and-criteria> on 14 January 2021

⁴⁵IATA-UPU Mail Safety Guidelines-Recommendations to DPOs, retrieved from <https://www.iata.org/contentassets/15ee3a255dc447b886d9a7e91fa65dbe/mail-safety-requirements.pdf> on 15 May 2021

d. *safety programmes for supply chain – to enhance national security by preventing acts of unlawful interference.*⁴⁶

4.7.16 Furthermore, the UPU Postal security – Office of exchange and international airmail security S59, security standard for mail screening requires that at each office of exchange or airmail unit mail screening must be carried out. It is the responsibilities of DPO to carry out the screening.⁴⁷

4.7.17 If DPO contracts another person to handle their international mail, the DPO must put in place processes and platforms for the contracted person to comply. No additional screening is required for items weighing up to 500grams if security measures in UPU GENERAL SECURITY MEASURES S58 are adhered to by the DPO.

4.7.18 Items are to be screened in accordance with methods stipulated by National Civil Aviation Security Program (NCASP); namely: Explosive Detection Dog - EDD; Explosive Detection System - EDS; Explosive Trace and Vapour Detection (ETVD); manual search; metal detection; X-Ray equipment or other wave-based systems. The method employed must sufficiently ensure that no prohibited articles are concealed in the item otherwise, the item will be rejected for conveyance.⁴⁸

4.7.19 Training, collaboration, and awareness programmes (for internal staff and customers) are very central to the four (4) aspects provided above. Whether accepting or not accepting the exceptions dangerous goods, the guideline encourages DPOs to have in place procedures for controlling the introduction

⁴⁶ IATA-UPU Mail Safety Guidelines-Recommendations to DPOs, retrieved from <https://www.iata.org/contentassets/15ee3a255dc447b886d9a7e91fa65dbe/mail-safety-requirements.pdf> on 15 May 2021

⁴⁷ UPU Postal security – Office of exchange and international airmail security S59, retrieved from <https://www.upu.int/en/Postal-Solutions/Programmes-Services/Postal-Supply-Chain/Security> on 18 January 2022

⁴⁸ UPU Postal security – Office of exchange and international airmail security S59, retrieved from <https://www.upu.int/en/Postal-Solutions/Programmes-Services/Postal-Supply-Chain/Security> on 18 January 2022

of dangerous goods into their postal networks in order keep the mail safe and secure.⁴⁹

Question 15: Do you think schedule B of the regulations is relevant and in line with the market changes?

Question 16: Do you think the Authority should continue to prescribe the list of prohibited and dangerous goods or leave it to conveyors?

Question 17: Do you think there are any other interventions that should be applied to avert the risk of dangerous goods in their postal systems?

4.8 CYBERSECURITY

4.8.1 Every organisation connected to the internet is a target for cyber intrusion activity and post offices are no exemption as they extend their business platforms to online. The postal services include storing consumers personal information that includes names, addresses/location, history of online shopping if shipping has been through the postal networks and connection with other people.

4.8.2 Cybercrime in postal sectors has been experienced when criminals looking to commit fraud and identity theft using mail scams such as fake cheques and money orders; offers on lottery winning scams, offers on work from home packages etc. to unsuspecting victims through the post. The question of how to combat fraudulent postings and mail scams remains a critical agenda to the security of postal operations.

⁴⁹ IATA-UPU Mail Safety Guidelines Recommendations to DPOs, retrieved from <https://www.iata.org/contentassets/15ee3a255dc447b886d9a7e91fa65dbe/mail-safety-requirements.pdf> on 15 May 2021

- 4.8.3 The postal sector needs to build capabilities to improve the resilience and security of digitalised postal processes and services. Lack of security can be detrimental to postal operators as there may be occurrence of theft of valuable information on the organisation itself and its customers.⁵⁰
- 4.8.4 The United States Postal Services (USPS) was hacked in 2014, the breach affected around 75,000 postal employees (current and retired) and confidential information for 2.9 million customers was compromised.⁵¹ Australia Post has also reported cyber incidents.⁵² Although attacks may not be serious enough to bring operations to a standstill, they affect the integrity of the postal services and sometimes severely impact postal operations costs.
- 4.8.5 In South Africa, the National ICT white paper promotes digitisation of services and platforms in order “to promote economic growth, development and competitiveness; drive the creation of decent work; and support local, national and regional integration”.⁵³
- 4.8.6 For a business to provide its offering over a digitised platform, it must be aware of the following pieces of legislation: The Electronic Communications and Transactions Act 25 2002 (“ECTA”) is the primary legislation to regulates electronic communications and transactions, the use of electronic signatures and develop a safe, secure environment for consumers.
- 4.8.7 The National Cybersecurity Policy Framework, 2015 (Government Gazette No. 39475) (“NCPF”) provides a national framework to deal with cybersecurity

⁵⁰ Retrieved from https://about.usps.com/publications/pub166/pub166_v04_revision_112019_tech_012.htm on 13 May 2021

⁵¹ Retrieved from <https://edition.cnn.com/2014/11/10/politics/postal-service-security-breach/index.html> on 23 April 2021

⁵² Barbaschow, A. AusPost reported 300 cyber incidents this year, but nothing to cause major disruption, retrieved from <https://www.zdnet.com/article/auspost-reported-300-cyber-incidents-this-year-but-nothing-to-cause-major-disruption/> on 23 April 2021

⁵³ National Integrated ICT White Paper Policy, retrieved from [National Integrated ICT Policy White.pdf \(dtps.gov.za\)](https://www.dtps.gov.za/National_Integrated_ICT_Policy_White.pdf) on 19 January 2022

matters. It acknowledges that ICTs are indispensable in modern society and recognises the challenge that cyberspace poses for the government.⁵⁴

4.8.8 The NCPF intends to “create a secure, dependable, reliable and trustworthy cyberenvironment that facilitates protection of critical information infrastructure while strengthening shared human values and understanding of cybersecurity in support of national security imperatives and the economy.”⁵⁵

4.8.9 The NCPF identifies the Justice Crime Prevention and Security Cluster (JCPS) working in consultation with other government clusters to oversee and implement this policy. The NCPF further establishes the Cybersecurity Hub and additional Computer Security Incident Response Teams (CSIRTs) to identify and record cybersecurity threats working in co-ordination with various industries. The NCPF calls different industries (telecoms, health, education, etc.) to create their CSIRTs which will identify cyberthreats and share information and interventions to prevent such.

4.8.10 In order to complete an electronic transaction a consumer exchanges personal information that may be stored on the e-commerce provider’s platform for a sometime. In this regard, promotion of protection of personal information is enshrined in the Protection of personal information Act, 2013 (Act No. 4 of 2013) (“POPIA”).

4.8.11 POPIA sets minimum requirements for the processing of personal information and regulate the flow of personal information across the borders of the Republic.⁵⁶ It holds accountable the responsible party collecting personal information to keep the information safe by putting in place security measures on the information integrity and confidentiality and to process the

⁵⁴ National Cybersecurity Framework, retrieved from https://www.gov.za/sites/default/files/gcis_document/201512/39475qon609.pdf on 20 January 2022

⁵⁵ Retrieved from [National Cybersecurity Policy Framework \(www.gov.za\)](https://www.gov.za) on 20 January 2022

⁵⁶ Retrieved from <https://www.gov.za/documents/protection-personal-information-ac> on 20 January 2022

information lawfully without compromising privacy of the data subject. Processing of such information must be with consent of the data subject and they have the right to object to data processing.

4.8.12 Additionally, the Cybercrimes Act, 2020 (Act No. 19 of 2020) ("Cybercrimes Act") intends to create offences which have a bearing on cybercrime and criminalise the disclosure of data messages which are harmful.⁵⁷

4.8.13 Cybercrime offenses found in the Cybercrimes Act include unlawful access and interception of data, cyber forgery, cyber extortion and malicious communications. These offenses are punishable to a penalty and/or jail sentence of between one (1) to fifteen (15) years in prison if convicted. Furthermore, the Cybercrime Act imposes obligations to report cybercrimes and directs the National Director of Public Prosecutions to keep statistics on the number, and results of prosecutions for the following cybercrimes: ⁵⁸

4.8.14 Section 3 (4) states that the Interception of data to be is the following:

"the acquisition, viewing, capturing or copying of data of a non-public nature through the use of a hardware or software tool contemplated in section 4(2) or any other means, so as to make some or all of the data available to a person, other than the lawful owner or holder of the data, the sender or the recipient or the intended recipient of that data, and includes the—

(a) examination or inspection of the contents of the data; and

(b) diversion of the data or any part thereof from its intended destination to any other destination".⁵⁹

4.8.15 Section 8 defines Cyber fraud as:

⁵⁷ Cybercrimes Act 19 of 2020, retrieved from <https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000> on 20 January 2022

⁵⁸ Cybercrimes Act 19 of 2020, retrieved from <https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000> on 20 January 2022

⁵⁹ Cybercrimes Act 19 of 2020, retrieved from <https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000> on 20 January 2022

"Any person who unlawfully and with the intention to defraud makes a misrepresentation—

(a) by means of data or a computer program; or

(b) through any interference with data or a computer program as contemplated in section 5(2)(a), (b) or (e) or interference with a computer data storage medium or a computer system as contemplated in section 6(2)(a), which causes actual or potential prejudice to another person, is guilty of the offence of cyber fraud."⁶⁰

4.8.16 In terms of section 9 (1) Cyber forgery and uttering is:

"Any person who unlawfully and with the intention to defraud makes—

(a) false data; or

(b) a false computer program, to the actual or potential prejudice of another person, is guilty of the offence of cyber forgery.

(2) Any person who unlawfully and with the intention to defraud, passes off—

(a) false data; or

(b) a false computer program, to the actual or potential prejudice of another person, is guilty of the offence of cyber uttering."⁶¹

4.8.17 Cyber extortion, which is dealt with in section 10, is defined as:

" Any person who unlawfully and intentionally commits or threatens to commit any offence contemplated in section 3(1), 5(1), 6(1) or 7(1)(a) or (d), for the purpose of—

(a) obtaining any advantage from another person; or

⁶⁰ Cybercrimes Act 19 of 2020, retrieved from <https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000> on 20 January 2022

⁶¹ Cybercrimes Act 19 of 2020, retrieved from <https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000> on 20 January 2022

*(b) compelling another person to perform or to abstain from performing any act, is guilty of the offence of cyber extortion.*⁶²

4.8.18 Malicious communication can occur in three (3) ways listed below:

4.8.18.1 Section 14 defines data messages which incites damage to property or violence as:

“Any person who discloses, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite—

(a) the causing of any damage to property belonging to; or

*(b) violence against, a person or a group of persons, is guilty of an offence.*⁶³

4.8.18.2 In terms of section 15 Data message which threatens persons with damage to property or violence is defined as:

“A person commits an offence if they, by means of an electronic communications service, unlawfully and intentionally discloses a data message, which—

(a) threatens a person with—

(i) damage to property belonging to that person or a related person; or

(ii) violence against that person or a related person; or

(b) threatens a group of persons or any person forming part of, or associated with, that group of persons with—

(i) damage to property belonging to that group of persons or any person forming part of, or associated with, that group of persons; or

⁶² Cybercrimes Act 19 of 2020, retrieved from <https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000> on 20 January 2022

⁶³ Cybercrimes Act 19 of 2020, retrieved from <https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000> on 20 January 2022

(ii) violence against the group of persons or any person forming part of, or associated with, that group of persons, and a reasonable person in possession of the same information, with due regard to all the circumstances, would perceive the data message, either by itself or in conjunction with any other data message or information, as a threat of damage to property or violence to a person or category of persons contemplated in paragraph (a) or (b), respectively.”⁶⁴

4.8.18.3 Section 16 states the following regarding disclosure of data message of intimate image:

“(1) Any person (“A”) who unlawfully and intentionally discloses, by means of an electronic communications service, a data message of an intimate image of a person (“B”), without the consent of B, is guilty of an offence.”⁶⁵

4.8.19 The UPU has approved several policy recommendations⁶⁶ for the postal sector cybersecurity framework.⁶⁷

- a. Policy 1: adoption of the Domain Name System Security Extension (DNSSEC)- provides a way for software to verify the origins of domain name system (DNS) data and check that it has not been modified in transit or by intermediaries. This is achieved by incorporating public key cryptography into the DNS hierarchy, forming a chain of trust originating at the root zone.⁶⁸

⁶⁴ Cybercrimes Act 19 of 2020, retrieved from <https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000> on 20 January 2022

⁶⁵ Cybercrimes Act 19 of 2020, retrieved from <https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000> on 20 January 2022

⁶⁶ Retrieved from <https://www.upu.int/en/Universal-Postal-Union/Activities/Digital-Services/-POST-Domain/Security-policy> 15 April 2021

⁶⁷ Retrieved from <https://www.upu.int/en/Universal-Postal-Union/Activities/Digital-Services/UPU-CYBERSECURITY-FRAMEWORK> on 15 April 2021

⁶⁸ UPU .POST DNSSEC implementation policy, retrieved from [https://www.upu.int/UPU/media/upu/files/UPU/activities/Digital%20Services/.post%20domain/DNSSEC-Policy-1-2-\(2021\).pdf](https://www.upu.int/UPU/media/upu/files/UPU/activities/Digital%20Services/.post%20domain/DNSSEC-Policy-1-2-(2021).pdf) on 04 August 2021

- b. Policy 2: secure email server - to help reduce the potential for e-mail-based abuse, such as e-mail spoofing and phishing e-mails. The e-mail and DNS server should be secured in accordance with the following four (4) principles:
- i. Do not use open relay; enable SMTP authentication.
 - ii. Activate reverse DNS lookup on the e-mail server.
 - iii. Enable Domain Keys Identified Mail (1024-bit key signature) (DKIM).
 - iv. Implement a Sender Policy Framework.⁶⁹
- c. Policy 3: Transport Layer Security (TLS) certificate and no redirection
- Transport Layer Security (TLS) is an "open standard for encryption which enables people and applications to communicate in private over the internet. It provides three essential services to help ensure security on the Internet:
- i. Message confidentiality,
 - ii. Authentication,
 - iii. Message integrity"⁷⁰

4.8.20 In addition to the TLS certificate, the UPU Post recommends a no redirection policy which helps to avoid misuse and hijacking of online information.⁷¹ This policy assists prevent attackers sent crafted links to users to direct them to the controlled fake login page.⁷²

4.8.21 Protection of personal information is also critical as the post office collects and maintain personal data sets. Article 10 of the UPU convention manual provides that:

⁶⁹ UPU .POST DNSSEC implementation policy, retrieved from [https://www.upu.int/UPU/media/upu/files/UPU/activities/Digital%20Services/.post%20domain/DNSSEC-Policy-1-2-\(2021\).pdf](https://www.upu.int/UPU/media/upu/files/UPU/activities/Digital%20Services/.post%20domain/DNSSEC-Policy-1-2-(2021).pdf)

⁷⁰ UPU .POST DNSSEC implementation policy, retrieved from [https://www.upu.int/UPU/media/upu/files/UPU/activities/Digital%20Services/.post%20domain/DNSSEC-Policy-1-2-\(2021\).pdf](https://www.upu.int/UPU/media/upu/files/UPU/activities/Digital%20Services/.post%20domain/DNSSEC-Policy-1-2-(2021).pdf)

⁷¹ Retrieved from <https://www.upu.int/en/Universal-Postal-Union/Activities/Digital-Services/-POST-Domain/Security-policy> on 04 August 2021

⁷² No-redirections for .POST domains, retrieved from https://www.upu.int/UPU/media/upu/files/UPU/aboutUpu/cooperativesAndBoards/.postGroupBoard/POC_DPG_GA_2022-1_Doc08_An03_clean.pdf on 19 January 2022

- a. "Personal data on users may be employed only for the purposes for which they were gathered in accordance with applicable national legislation.
- b. Personal data on users shall be disclosed only to third parties authorised by applicable national legislation to access them.
- c. Member countries and their designated operators shall ensure the confidentiality and security of personal data on users, in accordance with their national legislation.
- d. Designated operators shall inform their customers of the use that is made of their personal data, and of the purpose for which they have been gathered.
- e. Without prejudice to the foregoing, designated operators may transfer electronically personal data to the designated operators of destination or transit countries that need these data in order to fulfil the service".⁷³

4.8.22 CRASA guideline encourages postal and courier service providers to develop and operationalise comprehensive cybersecurity policies that seek to protect and safeguard the organisation's IT infrastructure.⁷⁴

4.8.23 The guideline further calls for the establishment of national Cyber Incident Response Team (CIRTs) by individual Member States, to be responsible for responding to security policy breaches and other cybersecurity incidents at national level. The teams must include postal experts. Threats and vulnerabilities associated with the sector to be considered within the scope of the mandate of the National CIRTs.⁷⁵

⁷³ Retrieved from <https://www.upu.int/en/Universal-Postal-Union/About-UPU/Acts#non-permanent-acts> on 04 August 2021

⁷⁴ CRASA guideline on postal Cybersecurity, retrieved from <https://www.crasa.org/crasa-publication/cat/35/postal-regulatory-guidelines/> on 15 April 2021

⁷⁵ CRASA guideline on postal Cybersecurity. retrieved from <https://www.crasa.org/crasa-publication/cat/35/postal-regulatory-guidelines/> on 15 April 2021

The Regulations do not make a provision for cybersecurity crimes during mail conveyance.

Question 18: What measures should the Authority consider in addressing cybersecurity crimes?

Question 19: Do you think the Authority should prescribe minimum cybersecurity measures in line with the UPU and CRASA guidelines?

4.9 MONITORING AND ENFORCEMENT

4.9.1 The Authority is empowered by Section 4 (3) (b) of the ICASA Act to monitor the postal services sector. Section 17F (1) of the ICASA Act requires the Authority to appoint inspectors to perform the functions provided for in the Act. Section 17G of the ICASA Act empowers the inspectors to enter the premises, search and seize. Monitoring compliance with these Regulations, includes postal inspectors conducting random visits to the conveyors' premises to conduct physical inspections.

4.9.2 In terms of regulation 4.3 the conveyor has a duty to publish information on how to deal with dangerous goods and prohibited substances at their outlets. Regulations 7 and 8 also require conveyors, for the benefit of the consumers, to publish a list of dangerous and all goods prohibited from being conveyed through the mail.

4.9.3 Some conveyors (particularly unreserved postal service operators) do not publish information on how to deal with dangerous goods and prohibited substances in their outlets. The conveyors argument is that their business model does not include consumers physically visiting their outlets for business,

however, this information is published on the conveyor's websites which are their primary platforms of conducting business.

- 4.9.4 Regulation 5.3 obliges the conveyor to be liable for any damage, loss and theft of mail from the point of receipt of the goods until the delivery of the goods is completed. Some conveyors include business terms and conditions which are not in line with these regulations when dealing with customers, i.e., including indemnity clauses in their waybill to refuse liability. The Authority has received complaints from consumers wherein conveyors have refused to accept liability for damages, lost and stolen mail items during conveyance. Such refusal is as a result of indemnity clauses in the waybill.
- 4.9.5 On security of mail, the regulation 6.1 (a) enjoins the conveyor to maintain a strict access control measures to safeguard the area where mail is kept. The measures must include but not limited to installation of security alarm systems and locking high value items. Some conveyors have failed to fully comply with these requirements. In some instances, conveyors have dysfunctional security alarms, and high value items not locked as per the Regulations.
- 4.9.6 Regulation 6.1 (b) requires the conveyor, through a register, to maintain proper and accurate records of the amount of mail processed. Complying with this requirement has been a challenge for some conveyors. During routine compliance visits, inspectors have found that a proper register is not maintained by some conveyors. The absence of proper register negatively impacts the process to follow up and resolve consumer complaints and compromises the safety of mail.
- 4.9.7 The argument against relying on the physical register only is that the postal services sector has moved to digital operations and thus requirements like keeping a register should encompass an online register.

4.9.8 Regulation 6.1 (d) requires a conveyor to develop and submit a six-monthly reviewed and updated security procedures for handling mail to the Authority within 1(one) month after the end of the financial year and 6 (six) months thereafter. Several conveyors do not submit updated security procedures for handling mail.

4.9.9 Schedule A of the Regulations provides a list of dangerous goods that are restricted to be conveyed through mail. Schedule B of the Regulations provide a list of prohibited goods restricted to be conveyed through mail. However, during inspection the Authority has come across dangerous and prohibited goods in conveyance. The Authority has also received complaints relating to prohibited items conveyed through mail.

Question 20: Do you think the Authority should make it compulsory for the conveyors to maintain a digitised register?

Question 21: Should the Authority review the frequency for the submission of updated security procedures for handling mail?

Question 22: Do you think the Authority should extend the requirement for conveyors to publish the information at the outlets to include publishing information on official digital platforms (i.e. website)?

Question 23: Do you think the measures provided in the Regulations, on liability for damage and loss of mail items, are enough to protect the consumer? If the answer is no, what additional measures do you suggest.

Question 24: Do you think the measures provided in the Regulations, on liability for damage and loss of mail items, are enough to protect the conveyors from false claims? If the answer is no, what additional measures do you suggest the Authority considers?

4.10 CONTRAVENTIONS AND PENALTIES

4.10.1 Article 9 of the UPU Convention Manual stipulates that member countries must adopt the necessary measures to prevent, prosecute and punish any person found guilty of the insertion in postal items any of the listed prohibited items including narcotics and psychotropic substances, as well as dangerous goods.⁷⁶

4.10.2 Although the UPU does not provide guidance on contraventions of specific regulations in this regard, the Authority is guided by the PSA on mail conveyance contraventions. For all other contraventions related to conveyance of mail, there are relevant legislation. For instance, the Cybercrime Act specifically guides on contraventions of mentioned cybercrimes and provides a penalty set upon conviction.

4.10.3 For mail conveyance contraventions, Regulation 9 states that *"Upon a determination of non-compliance by the Complaints and Compliance Committee ("CCC") in terms of the ICASA Act, the Authority may impose a fine not exceeding:*

- (a) *R250 000 on a conveyor who fails to comply with regulations 4, 5 and 6.1(a)*
- (b) *R150000 on a conveyor who fails to comply with regulations 6.1 (b), (c), (d), 6.2, 7 and 8."*

Question 25: Do you consider the penalties in the Regulations to be effective, if not, is there a need to introduce further penalties?

⁷⁶ UPU convention Manual, retrieved from <https://www.upu.int/UPU/media/upu/files/UPU/aboutUpu/acts/manualsInThreeVolumes/actInThreeVolumesManualOfConventionMaj1En.pdf> on 5 August 2021

5 SECTION D

5.1 INTERNATIONAL BENCHMARKING

5.1.1 This section provides information collected from different countries, under the themes of the conveyance of mail regulation. Countries were chosen according to the level of availability and accessibility of information and developments in the postal sector. The selected countries also provide a combination of postal services sector information from a developed to a developing economies perspective and are signatories to the UPU. The developed economies are the United States of America and United Kingdom. The developing economies are Malaysia, Zimbabwe and Tanzania.⁷⁷

5.1.2 Furthermore, this section has looked at different approaches in the regulation of conveyance of mail to assess the possible areas of improvement for South Africa. The benchmark follows the themes from the Regulations as presented in section D above. Where information is not available under such theme, this section will not present a discussion.

5.2 MALAYSIA

5.2.1 Malaysia is an emerging Asian economy on a transition towards a technology-driven and high-tech production-based pattern of development. Malaysia's total population in 2022 has increased by 0.2% to an estimated 32.7 million from 32.6 million in 2021.⁷⁸ Malaysia is one of the most open

⁷⁷ World Economic Situation and Prospects, 2014. retrieved from https://www.un.org/en/development/desa/policy/wesp/wesp_current/2014wesp_country_classification.pdf on 12 August 2022

⁷⁸ The Malaysian Reserve - Malaysia's total population reaches 32.7m, retrieved from <https://themalaysianreserve.com/2022/07/29/malaysias-total-population-reaches-32-7m/> on 22 July 2022

economies in the world with a trade to Gross Domestic Product ("GDP") ratio averaging over 130% since 2010.⁷⁹

- 5.2.2 Pos Malaysia Berhad ("Pos Malaysia") is the designated operator and the courier market provides a highly competitive service with dominance of providers such as FedEx, DHL (Dalsy Hillblom & Lynn), Deutsche Post Group, TNT (Thomas Nationwide Transport) and UPS (United Parcel Service).
- 5.2.3 The Postal Services Act 2012 ("ACT 741") of Malaysia provides for the licensing of postal services and the regulation of the postal services industry. The ACT 741 also provides for incidental or connected matters.⁸⁰ Postal regulation in Malaysia is provided by Malaysian Communications and Multimedia Commission ("MCMC") as legislated by the Act 741.⁸¹
- 5.2.4 According to section 10 of Act 741, the Minister has the power to grant licenses for both universal service and non-universal service providers for provision of postal services. The Minister may further impose conditions to the license, and she/he deems fit as per Section 13 (3) of Act 741.⁸²
- 5.2.5 MCMC may designate a body to be known as the 'Postal Forum' functioning as a consumer protection unit handling complaints, making recommendations to the MCMC and promoting consumer interests on consumer issues including tariffs, service standards; develop code of practise for postal services and to carry out any functions as may be determined by the MCMC.⁸³

⁷⁹ The World Bank in Malaysia, retrieved from <https://www.worldbank.org/en/country/malaysia/overview> on 22 July 2022

⁸⁰ Postal Services Act 2012 [Act 741], retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741> on 20 April 2021

⁸¹ Retrieved from <https://www.mcmc.gov.my/en/about-us/history> on 20 April 2021

⁸² Postal Services Act 2012 [Act 741], retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741> on 20 April 2021

⁸³ Postal Services Act 2012 [Act 741], retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741> (Section 50) on 20 July 2022

5.2.6 Association of Malaysian Express Carrier (AMEC) was appointed by MCMC in 2020 to undertake the role of managing the Postal Forum in terms of the Section 49 of Act 741.⁸⁴ Postal and express delivery services companies operating in Malaysia can apply for ordinary or associate membership whereby Ordinary membership is for USO providers and Associate membership is open to organisations that undertakes to provide services related to postal and express delivery, logistics, transportation, freight forwarders in Malaysia.⁸⁵

5.2.7 Definitions

5.2.7.1 Section 2 of Act 741 defines mail conveyance terms including post and postal article among others. The terms are defined as follows:

"post" means an act of leaving a postal article in any place, receptacle, device or mail conveyance of a licensee or with any person authorized by a licensee for the collection of postal articles and in the case of the universal service licensee, also means leaving it in any post office or depositing it in any posting box;

"postal article" means a letter, a package, a parcel, a wrapper or a container that can be collected, transmitted and delivered through the postal network of a licensee;

"mail conveyance" means the mode used to transmit postal articles;

"transmission of postal article" means the process whereby a postal article is being posted by the sender to an access point until it is being delivered to the addressee by the licensee or it is returned to the sender or disposed of under this Act by the licensee;

⁸⁴ Information on AMEC and the Postal Forum and/or guidelines and rules for consumer complaints handling is not available.

⁸⁵ Retrieved from <https://amec.my/aboutus.html> on 22 July 2022

"postal services" means the collection, transmission and delivery of any postal article;

"postal network as "the system of organization and resources in any form or manner used by a licensee in carrying out its operations including the aspects of the system used for -

- (a) collecting postal articles from the access points;*
- (b) handling and transporting postal articles from the access point*
- (c) processing the postal articles; and*
- (d) distributing the postal articles to the addressee."⁸⁶*

"postal network facilities which refers to "any facilities and equipment used by a licensee as part of its postal network and in the case of a universal service licensee includes a post office, posting box, relay box and postal vehicle; distribution Centre".⁸⁷

Malaysia defines key mail conveyance terms, i.e. post and mail conveyance, that are not defined in the Regulations.

Question 26: Should the Authority adopt Malaysia's definition of "post"?

Question 27: Should the Authority adopt Malaysia's definition of "mail conveyance"?

Question 28: What other definitions from Malaysia should the Authority consider adopting?

⁸⁶ Postal Services Act 2012 [Act 741], retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741> on 20 April 2021

⁸⁷ Postal Services Act 2012 [Act 741], retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741> on 20 April 2021

5.2.8 Scope

5.2.8.1 MCMC does not prescribe specific regulations on mail conveyance. However, mail conveyance activities are regulated by the Postal Services (Licensing) Regulations, 2015 and the Postal Services (Universal Service) Regulations, 2015. The former regulations provide licence conditions that are applicable to both universal and non-universal service providers,⁸⁸ while the latter regulations are only applicable to the universal service provider. The Universal Service Regulations provide clauses for purposes of postal services security as required by Section 101 (d) of the Act 741.⁸⁹

5.2.9 Duties and Powers of the Licensee

5.2.9.1 Duties and powers of the licensee are stipulated in various pieces of the following postal legislation. The Act 741 requires licensees to perform their duties and obligations as a universal or no-universal service provider. Licence applicants are required to develop and submit, to the MCMC, general terms and conditions including complaints handling procedure. They must publish information on delivery standards and charges and submit disaster recovery plan to MCMC.

5.2.9.2 Furthermore, Licensees are required to resolve consumer complaints before complaints are referred to MCMC.

5.2.9.3 The Act 741 requires a licensee to convey postal articles to the receiver without opening them. The licensee may open postal articles in case of satisfying the conditions under section 53 of the Act 741, which include, but not limited to; secure the contents or to ascertain the condition of the

⁸⁸ POSTAL SERVICES (LICENSING) REGULATIONS 2015, retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741/postal-services-licensing-regulations-2015> on 20 May 2021

⁸⁹ The Postal Services (Universal Service) Regulations, 2015, retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/postal_regulation2015_1.pdf on 12 August 2022

contents of damaged postal articles; or there are reasonable grounds to suspect that there is a physical danger to persons or property.

5.2.9.4 Where opened postal articles have been repacked, the licensee is required to maintain a record specifying all relevant details including but not limited to reason for opening, date, contents and employee who opened the postal article. The record shall be submitted upon request to the MCMC.

5.2.9.5 In addition, licensees are required to examine postal articles received from outside Malaysia.

5.2.10 Legal possession and ownership of mail

5.2.10.1 Act 741 does not make provision for when an article is considered in transmission of the postal network. However, under section 3 of Act 741, a postal article is considered delivered by the postal services licensee when “licensee:

- a. leave the postal article at the address;
- b. deposits the postal article in a post office locked bag or letter box or any other receptacle or device provided for the receipt of postal article of the addressee; or
- c. leaves the postal article with the addressee or his servant or agent or with any other person considered to be authorised by the addressee to receive the postal article, according to the usual manner of delivering postal article to that addressee, and where the addressee is a guest or a resident at a hotel, delivery to the proprietor or manager of the hotel or his agent shall be deemed to be delivery to the addressee”.⁹⁰

⁹⁰ Postal Services Act 2012 [Act 741], retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741> on 20 April 2021

5.2.10.2 Section 31 of the Act 741 provides an exemption for Pos Malaysia from liability for loss, mis-delivery, delay or damage as it states that: "A universal service licensee shall not be liable for any loss, mis-delivery, delay of or damage to the postal articles during the transmission of postal articles, unless it is proven that the universal service licensee has maliciously or negligently or intentionally cause the loss, mis-delivery, delay or damage."⁹¹ Clause 17 of the General Terms and Conditions for postal services ("GTC") support section 31 of ACT 741, except for the provision of complaint filing procedure, the GTC, does not provide the guidance and procedure to prove negligence.⁹²

5.2.11 Mail Safety

5.2.11.1 Postal Services (Licensing) Regulations, 2015, clause 9 (1) for universal service operators and clause 9 (2) for the non-universal service licensee requires that the licensee keep:

- a. maintenance of integrity of postal services at all times,
- b. submit its disaster plan for survival and recovery of any postal network facilities or postal service network in the event of a disaster to the MCMC, and
- c. Publication of its general terms and conditions including complaints handling procedure to consumers by any means.

5.2.11.2 In addressing maintenance of postal services integrity, Malaysia provides specific obligations only to the Universal service licensee. Clause 10 of the Postal Services (Universal Service) Regulations, 2015 provides that a universal service Licensee shall:

- "(a) take all reasonable measures to ensure the security of postal articles and postcards during the transmission of the postal articles and postcards;

⁹¹ Postal Services (Licensing) Regulations, 2015, retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741/postal-services-licensing-regulations-2015> on 20 May 2021

⁹² Retrieved from [Terms and Conditions - General \(pos.com.my\)](https://www.pos.com.my/terms-and-conditions-general) on 10 August 2022

- (b) implement reasonable security measures to protect the postal network facilities, postal employees and consumers; and
- (c) take all reasonable measures to ensure the postal employees, contractors and agents are fit and proper to carry out the provisioning of universal service".⁹³

5.2.12 Prohibited and Dangerous goods

5.2.12.1 The transmission of prohibited and dangerous goods is outlined in the general terms and conditions required to be prepared and submitted by licensees. Pos Malaysia publishes a list of prohibited and dangerous goods not to be transmitted through the postal network in line with UPU regulations and as defined by The International Air Transport Association ("IATA"), International Civil Aviation Organisation ("ICAO") and Civil Aviation Act which includes liquids, narcotics, flammables, radioactive and corrosives.⁹⁴

5.2.12.2 Pos Malaysia reserves the right to amend or change or modify or add or remove the classes of goods or Article which are categorised as Dangerous Goods or Prohibited Items at any time and from time to time without prior notice to customers.

5.2.12.3 Clause 4(d) of the GTC stipulates the right for Pos Malaysia to refuse transmission of dangerous and prohibited goods, furthermore, requires customers to declare contents of the postal article before acceptance into the postal network and extends liability "for any liabilities arising from any claims losses, fines, penalties, damages suffered or incurred by Pos Malaysia as a result of breach of this condition including but not limited to costs, fees, expenses, claims incurred in connection with the return,

⁹³ Postal Services (Universal Services) Regulations, 2015. retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/postal_regulation2015_1.pdf on 12 August 2022

⁹⁴ Retrieved from <https://www.pos.com.my/journal/dangerous-goods-prohibited-items-141.html> on 21 April 2021

disposal, destruction, seizure or detention of the Article and that a customer shall indemnify ".⁹⁵

5.2.12.4 Where conveyance of prohibited/dangerous goods is allowed, it will be transmitted under conditions that:

- a. all the necessary and required approvals from both the country of origin and the country of destination such items have been declared and accompanied by original supporting documents of the permission,
- b. are appropriately packed, marked and labelled according to the applicable rules.

5.2.12.5 Pos Malaysia may use its sole discretion to refuse providing the services and shall not be liable in any manner if the article is returned, destroyed or detained.

5.2.13 Cybersecurity

5.2.13.1 Like other postal operations, Pos Malaysia has been targeted by cybercriminals using fraudulent telephone calls, email and text messages with the intention to deceive, scam or steal (phish) personal and financial information.⁹⁶

5.2.13.2 Pos Malaysia reported to have detected an attempt of a malware attack to disrupt its operations in 2019 and therefore had to shut its online services and systems. In response to these attacks, Pos Malaysia is upgrading its systems regularly to rectify and restore systems.⁹⁷

5.2.13.3 Malaysia does not have only one piece of legislation addressing cybersecurity but has various pieces of legislation dealing with different

⁹⁵ Retrieved from [Terms and Conditions - General \(pos.com.my\)](#) on 10 August 2022

⁹⁶ Online Security, Fraud And Scams, retrieved from <https://www.pos.com.my/news-info/online-security-fraud-and-scams.html> on 21 April 2021

⁹⁷ Pos Malaysia takes proactive measures to secure systems following malware attack, retrieved from <https://www.marketing-interactive.com/pos-malaysia-takes-proactive-measures-to-secure-systems-following-malware-attack> on 21 April 2021

aspects of cybercrimes. The Digital Signature Act 1997 (DSA 1997) administered by the MCMC regulates the use of digital signature in Malaysia, ensures the security of legal issues related to electronic transactions and verifies the use of digital signatures through certificates issued by licensed Certification Authority (CA).

5.2.13.4 Personal Data Protection Act of 2010 (“PDPA”) is another piece of legislation used to address cybersecurity in postal services as it provides a comprehensive approach to issues of personal data protection across different sectors. The PDPA “regulates the processing of personal data in commercial transactions and applies to anyone who processes and has control over or authorises the processing of any personal data in respect of commercial transactions.”⁹⁸

5.2.13.5 In terms of section 16 of the PDPA, the postal services licensee is required to register with the Personal Data Protection Commissioner as a data user (“a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor”).⁹⁹ The registration certificate must be displayed at their principal place of business, and a copy of the certificate must also be displayed at each branch, where applicable. Failure to register is a punishable offence as per the provisions of the PDPA.¹⁰⁰

5.2.13.6 The PDPA obliges data users to obtain a data subject’s consent for the processing (which includes collection and disclosure) of personal data. The consent must be in a form that can be recorded and maintained by the Data User. Additionally, there is a requirement to notify data subjects regarding

⁹⁸ Official portal of Department of Personal Data Protection, retrieved from

<https://www.pdp.gov.my/jdpdv2/laws-of-malaysia-pdpa/background/?lang=en> on 5 August 2021

⁹⁹ Official portal of Department of Personal Data Protection, retrieved from <https://www.pdp.gov.my/jdpdv2/laws-of-malaysia-pdpa/interpretation/?lang=en> on 4 August 2021

¹⁰⁰ Retrieved from <https://www.pdp.gov.my/jdpdv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en> on 4 August 2021

the purpose for which their personal data are collected and a requirement to maintain a list of any personal data disclosures to third parties.¹⁰¹

5.2.13.7 The PDPA also establishes the Personal Data Protection Commissioner (“the Commissioner”) to oversee the registration of data users. Registration as a data user is valid for one year, after which, the data user can renew registration with the Commissioner. The Commissioner may cluster data users and data users are allowed to develop their own code of practice to govern compliance with the PDPA¹⁰².

5.2.13.8 Secondary to the PDPA, there is Personal Data Protection Regulation of 2013¹⁰³ which provides the seven principles a data user is to comply with and inspection process thereof.

5.2.13.9 Commissioner will from time to time publish the standards for following seven principles for data user to abide by:

- a. Consent – data user is required to attain consent from the data subject in relation to processing of personal data in any form that such data can be recorded and maintained properly,
- b. notice and choice – data subject must be provided at least with names and contacts of the designated person of the data user,
- c. disclosure - data user is required to keep a list of disclosure to third party in relation to personal data of subject data that is being processed,
- d. retention – data shall be retained as per standard issued by the commissioner,

¹⁰¹ Laws of Malaysia – Personal Data Protection Act, retrieved from <https://www.pdp.gov.my/jdpdv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en> on 4 August 2021

¹⁰² Laws of Malaysia – Personal Data Protection Act, retrieved from <https://www.pdp.gov.my/jdpdv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en> on 4 August 2021

¹⁰⁴ Personal Data Protection Act 2010 – Personal Data Protection Regulations, 2013 Retrieved from <https://www.pdp.gov.my/jdpdv2/assets/2019/09/LatestStandard.pdf> on 5 August 2021

- e. data integrity the commissioner will from time to time publish standards of integrity that data user must follow,
- f. Access – makes provisions for data access, correction and refusal requests by the data subject. It must be in writing and the data user must acknowledge request, and
- g. security principle - an organisation must ensure both technical and organisational security measures are well in place to safeguard the personally identifiable information that it processes.

5.2.13.9.1 The Personal Data Protection Standards of 2015 sets out the Commission's minimum requirements on the above principles for processing personal data electronically and non-electronically. The Standards include the following

- a. security standards – "A data user shall take practical steps to protect the personal data from any loss, misuse, modifications, unauthorized or accidental access or disclosure, alteration or destruction..."
- b. retention standards – "A data user shall take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed..."
- c. data integrity standards – "A data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept updated by having regard to the purpose, including any directly related purpose, for which the personal data was collected and processed further..."¹⁰⁴

5.2.13.9.2 In terms of data privacy, Pos Malaysia comply with the Personal Data Protection Act 2010. On its websites, Pos Malaysia publishes the Personal Data Protection Notice *which "outlines how Pos Malaysia collects, uses,*

¹⁰⁴ Personal Data Protection Act 2010 – Personal Data Protection Regulations, 2013 Retrieved from <https://www.pdp.gov.my/jdpdv2/assets/2019/09/LatestStandard.pdf> on 5 August 2021

*handles and protects the information and personal data given to them*¹⁰⁵. Furthermore, Pos Malaysia publishes tips on how customers can protect themselves and relevant cybercrime offices and contacts for reporting any suspected or committed cybercrime.¹⁰⁶

5.2.14 Contraventions and Penalties

5.2.14.1 The following contraventions and penalties are provided for in terms of Section 64 of the Act 741: penalties of unlawful acts (maliciously disposes of or destroys; opens; keeps, detains or hides; delays, abandons or misdirects; tampers with; or obstructs) against postal article in the course of its transmission. Upon conviction for such acts, a person will be liable to a fine not exceeding one hundred thousand ringgits (USD 23 609,97/ R349 491,90) or to imprisonment for a term not exceeding two years or to both.¹⁰⁷

5.2.14.2 Installation of access points without authorisation is a punishable offence and upon conviction, such person is liable to a fine not exceeding fifty thousand ringgits (USD 11 804,98/ R 174 621,70) or to imprisonment for a term not exceeding six months or to both as per section 66 of the ACT 741.¹⁰⁸

5.2.14.3 Another contravention is damage to postal network facilities. This is punishable with a fine not exceeding three hundred thousand ringgits (USD 70 829,91 / R1 048 449,30) or to imprisonment for a term not exceeding three years or to both.¹⁰⁹

¹⁰⁵Pos Malaysia Personal Data Protection Notice, retrieved from [Privacy Statement - Pos Malaysia](#) on 21 April 2021

¹⁰⁶ Pos Malaysia, Online Security fraud and scams, retrieved from <https://www.pos.com.my/news-info/online-security-fraud-and-scams.html> on 21 April 2021

¹⁰⁷ Postal Services Act 2012 [Act 741], retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741> on 12 August 2021

¹⁰⁸ Postal Services Act 2012 [Act 741], retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741> on 12 August 2021

¹⁰⁹ Postal Services Act 2012 [Act 741], retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741> on 12 August 2021

- 5.2.14.4 Affixing anything without authority to or disfiguring a postal network facility is also a punishable offence. Upon conviction, a person responsible is liable to a fine not exceeding ten thousand ringgits (USD 2 361,00 / R 34 948,61) or to imprisonment for a term not exceeding six months or to both.¹¹⁰
- 5.2.14.5 Lastly, no one is to tamper with official mark on a postal article, otherwise upon conviction, the person is liable to a fine not exceeding fifty thousand ringgits (USD 23 609,97/ R 349 491,90) or to imprisonment for a term not exceeding six months or to both.¹¹¹
- 5.2.14.6 In terms of data protection, failure to comply with the provisions in the PDPA may amount to a criminal offence. Failure to register with the commissioner as a data user, is an offence and punishable by a fine of up to 500, 000 ringgit (USD 118 147,44/R1 890 462,79 and/or imprisonment for up to two years. If any of the seven data protection principles are not complied with by the registered data users, a fine of up to 300,000 ringgits (USD 70 829,91/ R1 047 690,53) is payable and/or to two years imprisonment.¹¹²
- 5.2.14.7 Whereas, if person is convicted with unlawful collection, disclosure, and sale of personal data they will be liable to a fine of up to 500,000 ringgits (USD 118 049,85/R1 747 881,00) and/or up to three years imprisonment.¹¹³

¹¹⁰ Postal Services Act 2012 [Act 741], retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741> on 12 August 2021

¹¹¹ Postal Services Act 2012 [Act 741], retrieved from <https://www.mcmc.gov.my/en/legal/acts/postal-services-act-2012-act-741> on 12 August 2021

¹¹² Laws of Malaysia – Personal Data Protection Act, 2010. Retrieved from <https://www.pdp.gov.my/jpdpv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en> on 12 August 2021

¹¹³ Laws of Malaysia – Personal Data Protection Act, 2010. Retrieved from <https://www.pdp.gov.my/jpdpv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en> on 12 August 2021

5.3 TANZANIA

5.3.1 The United Republic of Tanzania ("Tanzania") is recorded as lower-middle-income country status by the world Bank reflecting a sustained macroeconomic stability. The World Bank estimates a real GDP growth rate of 4.3 percent and a GDP per capita growth rate of 1.3 percent in 2021.¹¹⁴ As of 2021, The population of Tanzania is estimated 61,498,438.¹¹⁵

5.3.2 The postal services in the United Republic of Tanzania are provided by the state- owned Tanzania Posts Corporation (TPC) as well as by a number of privately owned courier service companies, such as TNT, DHL and Sky Networks (Skynet).

5.3.3 Tanzania Postal Corporation ("TPC") is the country's designated postal operator governed by the Electronic Postal and Communications Act of 2010 ("EPOCA"). Section 44 (2) of the EPOCA charges TPC with responsibility for the transmission of postal items.

5.3.4 The EPOCA defines postal services as "postal services whose scope is determined and regulated by the Act, the objective is to ensure the collection, clearance, sorting, transmission, transportation and delivery of postal item."¹¹⁶

5.3.5 The postal market is delineated into two areas, reserved and unreserved. A reserved service area is applicable to letters and postcards of up to 500 grammes; packets and parcels of up to 10 kilogrammes and is designated as the Universal Postal Service (UPS) for the TPC. Other operators are licensed to operate in the unreserved area with different geographical area scope.

¹¹⁴ The World Bank in Tanzania, retrieved from <https://www.worldbank.org/en/country/tanzania/overview> on 22 July 2022

¹¹⁵ The World Bank in Tanzania, retrieved from <https://www.worldbank.org/en/country/tanzania/overview> on 15 August 2022

¹¹⁶ Electronic Postal and Communications Act of 2010, retrieved from <https://tanzlii.org/tz/legislation/act/2010/3-0> on 28 April 2021

5.3.6 The Tanzania Communications Authority (“TCRA”) is a governmental organisation established by the Tanzania Communications Regulatory Authority Act No.12 of 2003,¹¹⁷ responsible for regulations of the communications sector including postal services in Tanzania.

5.3.7 Definitions

5.3.8 Tanzania does not have a definition of the term mail conveyance but does define key terms within the mail conveyance space. The defined terms include, post, postal services, postal licensee network and postal article. The terms are defined in the following manner:

“post” means a system for collection, dispatch, conveyance, handling and delivery of postal articles by or through a public postal licensee;

“postal services” means postal services whose scope is determined and regulated by the Act with objective to ensuring the collection, clearance, sorting, transmission, transportation and delivery of postal item.

“postal licensee’s network” means all parts for those physical facilities involved in the activities of conveying, receiving, collecting, sending, dispatching and delivering letters within, to and from Tanzania by sea, land or by air or through any person with whom the licensee has a contract with or its agents or servants;

“postal article or postal item” means material goods with or without mercantile value, that comply with the post ability requirements determined by this Act and by regulation and are delivered via physical network to a specified address or a person with a specified address”.¹¹⁸

¹¹⁷ Retrieved from <https://www.tcra.go.tz/documents/legislation-1> on 28 April 2021

¹¹⁸ Retrieved from <https://tanzlii.org/tz/legislation/act/2010/3-0> on 28 April 2021

5.3.9 Scope

5.3.9.1 Tanzania does not have specific regulations on conveyance of mail however, the Electronic and Communications (Postal) Regulations, 2018 ("Postal Regulations 2018") are utilised in regulating mail conveyance.¹¹⁹ The Postal Regulations 2018 apply to postal and courier services.

5.3.10 Duties and Powers of the Postal Licensee

5.3.10.1 Tanzania does not have specific regulations on mail conveyance, duties and powers of the conveyors are stipulated in various pieces of the following postal legislation.

5.3.10.2 Section 42 of the EPOCA entrusts the postal licensees with the responsibility to handle, with integrity and not violate the secrecy, any correspondence of postal items deposited to the mailing system. Correspondence and other postal items may legally be opened only in exceptional circumstances expressly established under this section for reasons of verification and control by competent police, senior staff of the TCRA or customs and revenue officials.¹²⁰ Such officials have powers to destroy any postal items and materials containing prohibited items and stopped them from been dispatched.

5.3.10.3 Postal Regulations 2018 requires that "each licensee must ensure that steps are taken to improve mail security and combat postal crimes.¹²¹ A postal licensee may refuse to accept correspondence or postal item that doesn't fulfil the requirements established by the regulations. Clause 16 (1-6) of the Postal Regulations 2018 provides for procedure for parcel post which includes examination of the parcel by postal staff before transmission, description of the contents of the parcel; payments of any required

¹¹⁹ Retrieved from <https://www.tcra.go.tz/en/regulations> on 29 April 2021

¹²⁰ Retrieved from <https://tanzlii.org/tz/legislation/act/2010/3-0> 17 November 2021

¹²¹ Retrieved from <https://www.tcra.go.tz/en/regulations> on 29 April 2021

processes of transmission (e.g. customs) and subjected to security checks as defined by the UPU security standards.¹²²

5.3.10.4 The postal licensee is required to submit to TCRA their compensation policies for compensation of loss or damage of postal items. Section 51 (1)(d) of the EPOCA empowers TCRA to make rules to *provide for the payment of compensation for the loss or damage in course of transmission by post of postal articles, and the conditions under which such compensation may be paid and the limit of the amount of such compensation.*"

5.3.10.5 The Postal Regulation 2018 charges the postal licensee with the responsibility to pay compensation for loss or damage of postal items unless posted items are prohibited or over-insured; falsely stated; signed and returned without objection by the receiver and/or in case of apparent trace of theft or damage to the seal of the insured item.¹²³

Question 29: Should the Authority require conveyors to submit their compensation policies for compensation of loss or damage of postal items?

5.3.11 Legal Possession and Ownership of Mail

5.3.11.1 Section 44 (2) of EPOCA, provides that any *"correspondences and postal items which have been posted shall remain the property of the sender until final delivery to the addressee or to the displayed address, except when they are apprehended by a competent authority ."*¹²⁴

¹²² Retrieved from [https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20\(Postal\)%20Regulations.%202018](https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20(Postal)%20Regulations.%202018) on 28 April 2021

¹²³ Retrieved from <https://www.tcra.go.tz/documents/regulations> on 10 August 2022

¹²⁴ Retrieved from <https://tanzlii.org/tz/legislation/act/2010/3-0> on 28 April 2021

- 5.3.11.2 EPOCA and the Postal Regulations, 2018¹²⁵ provides for when postal article (hybrid or courier service) is posted and when it is considered delivered.
- 5.3.11.3 According to Section 44 (1) EPOCA, "A postal article shall be deemed to have been posted if it is deposited into a posting box or handed over to an employee or agent of a postal licensee authorized to receive it."¹²⁶
- 5.3.11.4 And "shall be deemed to have been received if it has been sent to the private letter box or private bag of the addressee or is left at the house or office of the addressee, or with the addressee, or with his employee, or agent, or other person authorized to receive it and, where the addressee is a guest or is resident at a hotel, hostel or lodging of a similar nature, if it is left with the proprietor or manager thereof or with his agent."¹²⁷
- 5.3.11.5 Hybrid mail "shall be deemed to have been posted when an electronic version has been transmitted to the postal licensee's network and delivered to the addressee when it is delivered by the Designated Postal Operator at his physical address or into his private box or bag operated at a post office or rural delivery box."¹²⁸
- 5.3.11.6 With regards to courier services, "a postal item shall be deemed to be delivered to the addressee when it is delivered by courier licensee at the customer's physical address or picked from a courier operator's counter."¹²⁹
- 5.3.11.7 The postal licensee is liable for compensation of lost, misplaced or correspondences or postal items. The postal licensee is liable to compensate the customer based on the rules made by the Authority as

¹²⁵ Retrieved from <https://www.tcra.go.tz/en/regulations> on 29 April 2021

¹²⁶ Retrieved from <https://tanzlii.org/tz/legislation/act/2010/3-0> on 28 April 2021

¹²⁷ Retrieved from <https://tanzlii.org/tz/legislation/act/2010/3-0> on 28 April 2021

¹²⁸ Retrieved from <https://www.tcra.go.tz/en/regulations> on 29 April 2021

¹²⁹ Retrieved from <https://www.tcra.go.tz/en/regulations> on 29 April 2021

provided by section 43 (1) and discussed in the above subsection (duties and powers).¹³⁰

5.3.11.8 Section 43 (3) EPOCA, provides an exception for postal licensee's liability to the customer for loss, misplaced, delayed delivery or failure to guarantee the integrity of correspondence or postal if that customer is "(a) owing to user behaviour involving an infringement of the law or regulation; and (b) owing to defects or risks inherent in the nature of correspondence or postal items."¹³¹

5.3.12 Dangerous and Prohibited Goods

5.3.12.1 Transmission of dangerous are prohibited to be transmitted by the postal network in Tanzania as stipulated in the EPOCA Act. Section 51 (1) (c) of the EPOCA empowers TCRA to make rules prohibiting the transmission by post of postal articles not specified in Section 46 or lay down special conditions on which such articles, may be transmitted by post.

5.3.12.2 The sender shall be liable to the postal licensee for any damage caused by failure to comply with the portability requirements established in this Act, except in cases of error or negligence by the postal licensee.

5.3.12.3 According to the Electronic and Postal Communications (Postal) Regulations, 2018, prohibited postal items may be exceptionally conveyed by the post in a manner set out in the Regulations Schedule.

5.3.12.4 Section 52(1) prohibits any posting of items that may injure or endangers any person or the postal network during the course of transmission, which may include (2) *explosive, inflammable, dangerous, filthy, noxious or deleterious substance, any sharp instrument not properly protected, or any*

¹³⁰ Retrieved from <https://tanzlii.org/tz/legislation/act/2010/3-0> on 28 April 2021

¹³¹ Retrieved from <https://tanzlii.org/tz/legislation/act/2010/3-0> on 28 April 2021

living creature which is either noxious or likely to injure any person or any postal article in course of transmission by post. Or (3) opium, morphine, cocaine or any narcotic except under such rules as the TCRA may make in this behalf, and(4) Nothing in this section shall affect the provisions of any written law relating to deleterious drugs.”¹³²

5.3.12.5 Section 54 requires that TCRA make rules for preventing the sending and delivery of articles prohibited under this Act and detaining, disposing of, or destroying any such postal article sent or tendered for transmission by post.

5.3.12.6 The Electronic and Postal Communications (Postal) Regulations, 2018, clause 20, describes the items that are prohibited for the transmission by post, however, does not put an obligation on the licensee to publish the list for the benefit of consumers.

5.3.12.7 Section 55 (1) of the EPOCA imposes an obligation on the postal licensee to inform and handover to the TCRA any goods suspected to be in contravention of the EPOCA Act or country laws of dangerous goods.¹³³

Question 30: Should the Authority require conveyors to keep an updated record of dangerous and prohibited goods found in their postal networks?

5.3.13 Mail Safety and Security

5.3.13.1 The National Postal Policy of Tanzania (2003) had identified Postal Security and Safety as a policy issue in order to attain optimum security and safety. The policy acknowledges the occurrences through on a decline of theft, violation and loss of mail items. However, the policy identifies increased

¹³² Retrieved from <https://www.tcra.go.tz/documents/regulations> on 10 August 2022

¹³³ Retrieved from <https://www.tcra.go.tz/documents/regulations> on 10 August 2022

threats from modern day terrorism, as well as the prohibited dissemination of narcotics contraband and other undesirable articles as major issues.¹³⁴

Section 51(1) of the EPOCA empowers TCRA to "*make particular rules to (a) provide for the performance of supplementary services in respect of transmission by post of postal articles; (2) supplementary services include the registration, insurance and storage of postal articles, Poste Restante and any other form of supplementary service.*"

5.3.13.2 In this regard, Clause 23 of the Postal Regulations 2018¹³⁵ requires that "each licensee to ensure that steps are taken to improve mail security and combat postal crimes which include:

- a. mail violation and secretion.
- b. mail bombs.
- c. illicit drug or firearms trafficking; and theft.
- d. damaging postal property.¹³⁶

5.3.13.3 Security measures implemented by the TPC include using the Closed-Circuit Television (CCTV) at Dar es Salaam Post Office to strengthen the surveillance of both international and domestic mails.¹³⁷ The Tanzanian Post invested more on personnel to beef up safety and security measures of mail and at the same time maintain a global quality standard.

5.3.14 Cybersecurity

5.3.14.1 Similar to other countries, Tanzania does not have a specific cybersecurity legislation for postal services. Various pieces of legislations are used to regulate cybersecurity crimes in the postal services sector.

¹³⁴ Retrieved from <https://www.tcra.go.tz/uploads/documents/sw-1619081572-National%20Postal%20Policy%202003.pdf> on 10 August 2022

¹³⁵ Retrieved from <https://www.tcra.go.tz/en/regulations> on 29 April 2021

¹³⁶ Retrieved from <https://www.tcra.go.tz/en/regulations> on 29 April 2021

¹³⁷ Retrieved from <https://www.ship24.com/couriers/tanzania-post> on 02 February 2022

- 5.3.14.2 The Electronic Transactions Act, 2015 provide for the legal recognition of electronic transactions to provide for the facilitation of use of secure electronic signatures and other related matters including consumer protection.
- 5.3.14.3 Cybercrimes Act of 2015 as amended, is the legislation that deals with the cybercrimes in Tanzania providing for matters such as data espionage, publication of false and deceptive, and provide for the investigation, collection and use of electronic evidence and matters related ¹³⁸
- 5.3.14.4 Section 124(1) of the EPOCA hereby “*establish a National Computer Emergency Response Team (CERT), which shall coordinate response to cyber security incidents at the national level and cooperate with regional and international entities involved with the management of cyber security incidents*”, and makes unauthorised access or use of computer system a punishable offense with liability to a fine not less than five hundred thousand Tanzanian shillings (R349700) or to imprisonment for a term of not exceeding three months or to both.
- 5.3.14.5 Section 42 of the EPOCA charges the postal licensee with the “*responsibility for the inviolability of the secrecy of correspondence and for the confidentiality and integrity of postal items.*” This ensures confidentiality of items under transmission of the TPC.
- 5.3.14.6 In terms of information privacy, clause 6(1) of the Electronic and Postal Communications (Consumer Protection) Regulations, 2018 requires that “a licensee may collect and maintain information on individual consumers where it is reasonably required for its business purposes.”¹³⁹ Such information collection and maintenance process must be “(a)*fair and lawful, (b)processed for identified purposes; (c) accurate; (d) processed in*

¹³⁸ Retrieved from <https://namati.org/resources/tanzania-cybercrimes-act-2015> on 03 February 2022

¹³⁹ Retrieved from [THE ELECTRONIC AND POSTAL COMMUNICATIONS ACT, 2010 \(tcr.go.tz\)](https://www.tcr.go.tz/) on 10 August 2022

accordance with the consumer's other rights; (e) protected against improper or accidental disclosure; and (f) not transferred to any party except as permitted by any terms and conditions agreed with the consumer,"¹⁴⁰

Question 31: In addition to the prescript of POPIA, should the Authority require mail conveyors to deal with personal information in a manner similar to Tanzania clause 6(1) of the Electronic and Postal Communications (Consumer Protection) Regulations, 2018?

5.3.15 Contraventions and Penalties

5.3.15.1 The EPOCA provides for the following contraventions and penalties in relation to mail conveyance: Section 148 provides offenses against *"any officer, employee or agent of a public postal licensee who destroys or throws away any postal articles in the course of transmission by post or anything contained therein"*¹⁴¹

5.3.15.2 Section 139 provides that: *"Any person who sends by post any postal article or anything which is injurious, indecent or prohibited item under section 42 (1),(3),section 45 and 46 of EPOCA and the Drug Control and Enforcement Act of 2015, respectively, commits an offence and shall, on conviction, be liable to a fine not exceeding less than not less than five million Tanzanian shillings (R318469.33) or to imprisonment for a term not less than twelve month or to both."*¹⁴²

¹⁴⁰ Retrieved from [THE ELECTRONIC AND POSTAL COMMUNICATIONS ACT, 2010 \(tcra.go.tz\)](https://www.tcra.go.tz) on 10 August 2022

¹⁴¹ Retrieved from [Microsoft Word - The Electronic and Postal Communications, Final HANSARD.doc \(tcra.go.tz\)](#) on 10 August 2022

¹⁴² Retrieved from [Microsoft Word - The Electronic and Postal Communications, Final HANSARD.doc \(tcra.go.tz\)](#) on 10 August 2022

5.3.15.3 Section 151 of the EPOCA provides that “Any person who willfully removes, destroys or damages any installation or plant used for postal or Electronic communication services commits an offence and shall be liable on conviction to a fine not less than one million shillings, or to imprisonment for a term not less than three years or to both.”¹⁴³

5.4 UNITED STATES OF AMERICA (USA)

5.4.1 United States of America (“USA”) is among the most developed countries, with a total GDP of \$20.95 trillion. It has a reported total population of 331,893,745.¹⁴⁴

5.4.2 United States Postal Services (“USPS”) is the designated postal operator of the USA.¹⁴⁵ It is mandated to provide universal services under the Postal Accountability and Enhancement Act of 2006 (“PAEA”). It is regulated under the Postal Regulatory Commission (“PRC”). The PRC is empowered to set prices for the postal services, set service performance standards, and monitor legislative compliance. USPS competes directly with the courier giants, FEDEX and UPS for delivery of urgent letters and parcels.

5.4.3 The US Postal Inspection Service is a federal law enforcement agency established to protect the Postal Service, secure the mail system, and ensure public trust in the mail.¹⁴⁶

5.4.4 The US Postal Inspection Service has investigative special agents stationed nationwide to focus on issues such as protection of employees, illegal narcotics, mail and package theft, identity theft, mail fraud, fraud prevention

¹⁴³ Retrieved from [https://www.tcra.go.tz/uploads/documents/en-1619082940-The%20Electronic%20and%20Postal%20Communications%20Act,%202010%20\(Act%20No.%203%20out%20of%2010\).pdf](https://www.tcra.go.tz/uploads/documents/en-1619082940-The%20Electronic%20and%20Postal%20Communications%20Act,%202010%20(Act%20No.%203%20out%20of%2010).pdf) on 10 August 2022

¹⁴⁴ Retrieved from <https://data.worldbank.org/country/US> on 22 July 2022

¹⁴⁵ Retrieved from [Postal Act of 2006 - What we do - About.usps.com](https://about.usps.com/publications/pub278/welcome.htm) on 10 August 2022

¹⁴⁶ Retrieved from <https://about.usps.com/publications/pub278/welcome.htm> on 19 April 2021

and education, suspicious mail, disaster response, money laundering, cybercrime and global mail security.¹⁴⁷

5.4.5 The US Postal Inspection Service is a federal law enforcement agency established to protect the Postal Service, secure the mail system, and ensure public trust in the mail.¹⁴⁸ Under the US Postal Inspection service, the Office of Inspector General (OIG) ensures the integrity of postal processes, finances, and personnel. The PRC is empowered by PAEA to select, appoint and employ officers and employees of the OIG of the Postal Regulatory Commission.

5.4.6 The OIG has investigative special agents stationed nationwide to focus on issues such as protection of employees, illegal narcotics, mail and package theft, identity theft, mail fraud, fraud prevention and education, suspicious mail, disaster response, money laundering, cybercrime and global mail security.¹⁴⁹ The PRC is empowered by Section 605 of PAEA to select, appoint, and employ officers and employees of the OIG of the Postal Regulatory Commission.

5.4.7 Definitions

5.4.7.1 US PAEA does not have a definition of the term mail conveyance, post and postal article. The following relevant terms postal service and non- postal service are defined in the following manner:

“postal service refers to the delivery of letters, printed matter, or mailable packages, including acceptance, collection, sorting, transportation, or other functions ancillary thereto;”¹⁵⁰

¹⁴⁷ Retrieved from <https://www.uspis.gov/about/what-we-do> on 23 April 2021

¹⁴⁸ Retrieved from <https://about.usps.com/publications/pub278/welcome.htm> on 19 April 2021

¹⁴⁹ Retrieved from <https://www.uspis.gov/about/what-we-do> on 23 April 2021

¹⁵⁰ Retrieved from [HR 6407 RDS - Postal Accountability and Enhancement Act - Postal Act of 2006 - What we do - About.usps.com](#) on 20 August 2022

“non-postal service means any service that is not a postal service defined *under section 102(5)*.” *These services shall be reviewed and designated by the PCR for regulation as a “ market dominant product, a competitive product, or an experimental product”,*¹⁵¹ described in the mail classification schedule.”¹⁵²

5.4.8 Scope

- 5.4.8.1 The USA does not have specific regulations for the conveyance of mail, however, presents rules and procedures (information) in the publications called USPS Guide to Mail Centre Security.¹⁵³
- 5.4.8.2 The latter provides information on who is responsible for guarding mail, risk assessment standards for mail operations; enhancing physical security for workplace and layout of the mail centre; mail theft; identifying right security plan for mail centre against dangerous and prohibited goods (bombs, chemical, biological and radiological threats) and handling and processing mail safely. The USPS Guide to Mail Centre Security scope is limited to only the USPS.

5.4.9 Powers and Duties

- 5.4.9.1 PAEA gives USPS the responsibility to provide frequent, reliable, safe and secure delivery of mail, packages and other communications throughout the country. USPS remains accountable to the PRC.

¹⁵¹ Retrieved from [HR 6407 RDS - Postal Accountability and Enhancement Act - Postal Act of 2006 - What we do - About.usps.com](#) on 20 August 2022

¹⁵² Retrieved from [Mail Classification Schedule \(MCS\) | Postal Regulatory Commission \(prc.gov\)](#) on 10 August 2022

¹⁵³ Retrieved from https://about.usps.com/publications/pub166/pub166_v04_revision_112019_tech_006.htm on 12 August 2021

5.4.10 Legal possession and ownership of mail

5.4.10.1 PAEA is not explicit in providing the powers of the USPS to legally possess mail in their system. However, the USPS Guide to Mail Centre Security,¹⁵⁴ asserts that protection for mail ends when items are removed by the addressee or the addressee's agent from the box. Mail received into the hands of an addressee or addressee's agent is considered properly delivered mail.¹⁵⁵

5.4.11 Mail safety and security

5.4.11.1 In terms of mail centre security, USPS Guide to Mail Centre Security¹⁵⁶ provides several actions and processes the USPS undertakes. The OIG conducts and recommends risk assessment of mail operations focusing on the physical location where mail is handled and its accessibility to employees and the public. Risk assessments include checking on:

- a. Location of mail operations;
- b. Jobs and tasks involved in processing mail;
- c. Personnel who handle the mail; and
- d. customers.¹⁵⁷

5.4.11.2 Enhancement of a physical layout for mail centre is recommended as a preventive security measure and reduce safety and security risk. USPS provides a detailed checklist to check mail centre security.¹⁵⁸

5.4.11.3 While physical layout security is recommended, mail centres are also more likely to experience problems caused by common crimes such as theft. Lack

¹⁵⁴ Retrieved from https://about.usps.com/publications/pub166/pub166_v04_revision_112019_tech_006.htm on 12 August 2021

¹⁵⁵ Retrieved from https://about.usps.com/publications/pub166/pub166_v04_revision_112019_tech_006.htm on 12 August 2022

¹⁵⁶ Retrieved from https://about.usps.com/publications/pub166/pub166_v04_revision_112019_tech_006.htm on 12 August 2021

¹⁵⁷ Retrieved from <https://about.usps.com/publications/pub166.pdf> on 23 April 2021

¹⁵⁸ Retrieved from [Enhancing the Physical Layout of Your Mail Center \(usps.com\)](https://www.usps.com/physical-layout) on 10 August 2022

of security can result in theft of supplies, postage, mail, and any valuable information about the Postal Service contained in sensitive mail.

- 5.4.11.4 The Postal Inspection Service recommends the development of screening procedures for all incoming deliveries, including those from private delivery companies.¹⁵⁹ Mail Conveyors must include training of all employees on safe mail handling procedures and understanding the importance of following protocols.¹⁶⁰
- 5.4.11.5 Information held by the Postal Inspection Service shows that mail theft reports soared by 600% over 2017 to 2020. It has been reported and acknowledge by the OIG that the US mail system has no reliable system for tracking mail theft.¹⁶¹
- 5.4.11.6 According to the Postal Inspection Service, the figures reflected multiple types of customer complaints, not only those involving theft. The system currently used by the USPS is limited to capturing all cases as theft and does not re-categorise other issues such as mailbox vandalism, mail delivery problems etc.¹⁶²
- 5.4.11.7 Other cases of mail theft reported include theft by mail employees stealing gift cards and cash from the mail.¹⁶³ The OIG is charged with the responsibility of identifying dishonest employees and take proper investigative steps to have them prosecuted and removed from the postal service. OIG is reported to have conducted, in 2019-2020, 1,221 internal mail theft investigations. This resulted in 333 arrests, 1,000 administrative

¹⁵⁹ Retrieved from https://about.usps.com/publications/pub166/pub166_v04_revision_112019_tech_015.htm on 24 April 2021

¹⁶⁰ Retrieved from <https://about.usps.com/publications/pub166.pdf> on 23 April 2021

¹⁶¹ Retrieved from <https://www.nbcnews.com/news/us-news/mail-theft-surg-ing-u-s-postal-service-inspectors-don-t-n1241179> on 11 November 2021

¹⁶² Retrieved from <https://www.uspsoidg.gov/investigations/internal-mail-theft> on 23 April 2021

¹⁶³ Retrieved from <https://apnews.com/article/postal-service-omaha-theft-crime-5629a21c9fa4005c6a9faff9095e8fea> on 23 April 2021

actions, and approximately \$588,000 in monetary benefit for the postal service.¹⁶⁴

5.4.11.8 In terms of addressing mail theft by employees, the OIG conducts employee screening process which includes conducting the interview, drug screening, and local criminal background check. There are further checks with the National Agency Check with Inquiries (NACI) once a person is employed with the USPS.¹⁶⁵

Question 32: Should the Authority outline items that should be included in the risk assessment register as the USPS Guide to Mail Centre Security?

5.4.12 Dangerous and prohibited goods

5.4.12.1 The PAEA prohibits material that has been declared hazardous by statute or Postal Service regulation to be nonmailable.¹⁶⁶ PAEA requires the USPS to produce guidelines for the safe transportation of hazardous material in the mail.

5.4.12.2 The USPS publishes on its website a guideline called "Publication 52 of Hazardous, Restricted and Perishable Mail". The guideline provides information and guidance for when mailing items that are prohibited (completely forbidden) and restricted (only allowed under certain conditions) to be in line with the UPU rules.¹⁶⁷ These items include:

- a. prohibited (corrosives; explosives; flammable liquids and solids, combustible liquids etc.),

¹⁶⁴ Retrieved from <https://www.uspsoidg.gov/investigations/internal-mail-theft> on 23 April 2021

¹⁶⁵ Retrieved from <https://www.uspsoidg.gov/document/nationwide-employee-background-screening> on 23 April 2021

¹⁶⁶ Retrieved from <https://www.prc.gov/sites/default/files/references/pl109-435paea.pdf> on 24 April 2021

¹⁶⁷ Retrieved from <https://www.usps.com/ship/shipping-restrictions.htm> on 23 April 2021

- b. restricted (abortive and contraceptive device, battery-powered devices, Building construction materials etc); and
- c. perishable Mail (dead animals or parts of animals, eggs, Live animals etc)¹⁶⁸

5.4.12.3 For anything to be considered non-mailable it should be because "it may kill or injure another or injure the mails or other property...". Restricted material is an article or substance prohibited or limited because it may, under conditions encountered in the mail, be injurious to life, health, or property.¹⁶⁹

5.4.12.4 The publication 52 guideline provides postal personnel with ways to handling and transport of hazardous materials, restricted matter, and perishable matter to protect themselves in line with the UPU General security measures S58 and UPU Postal Security – Office of exchange and international airmail security S59.¹⁷⁰ For instance, appendix C of the Publication 52 guideline, provides packaging instructions for hazardous material, quantity provisions, which test to undergo, mailable only for domestic, weighting and how outer packaging and labelling should be like.

5.4.13 Cybersecurity

5.4.13.1 Cybersecurity issues are addressed at both the federal and state levels by various legislations and vary by commercial sectors. The Children's Online Privacy Protection Act Of 1998 ("COPPA") intends to protect minors (13 years and under) by giving their parents the responsibility to give consent about the child for usage of programmes on internet.¹⁷¹ The COPPA is enforced by THE Federal Trade Commission ("FTC").

¹⁶⁸ Retrieved from <https://pe.usps.com/text/pub52/welcome.htm> on 23 April 2021

¹⁶⁹ Retrieved from <https://pe.usps.com/text/pub52/welcome.htm> on 12 August 2021

¹⁷⁰ Retrieved from <https://pe.usps.com/text/pub52/welcome.htm> on 12 August 2021

¹⁷¹ Retrieved from <https://www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online> on 12 August 2021

5.4.13.2 The Cybersecurity Information Sharing Act of 2015 (“CISA”) makes provision for the sharing of information for cybersecurity between and among the private sector; state, local, tribal, and territorial governments; and the Federal Government.¹⁷²

5.4.13.3 In addition, other states have passed their own cybersecurity laws. For instance, California Consumer Privacy Act (“CCPA”) is specifically for organisations operating in the California state. It also gives more powers to the consumers over their personal information that businesses want to collect about them.¹⁷³ For instance, consumers have the right:

- a. to know what information a business collects about them and how it is used and shared;
- b. to delete personal information collected from them;
- c. to opt-out of the sale of their personal information; and
- d. to non-discrimination for exercising their CCPA rights.
- e. Moreover, businesses are required to give consumers notices explaining their privacy practices.

5.4.13.4 With regards to the postal sector, the USPS 2019 report ¹⁷⁴ to the OIG, lists cybersecurity as one of the challenges facing the USPS. The Postal Inspection Office (“PIO”) has established a cybercrime unit to provide investigative, forensic, and analytical support to Inspection Service field divisions and the USPS by constantly monitoring the internet and dark web for cyber activity that abuses or attacks the U.S. Mail system.¹⁷⁵

5.4.13.5 The USPS Information Security handbook provides a “framework of information security policies to ensure the detection, prevention, response to, and investigation of cybercrime incidents and misuse of Postal Service

¹⁷² Retrieved from <https://www.cisa.gov/cybersecurity> on 12 August 2021

¹⁷³ Retrieved from <https://oag.ca.gov/privacy/ccpa> on 12 August 2021

¹⁷⁴ Retrieved from <https://www.oversight.gov/sites/default/files/oig-sa-reports/fall-2019-semiannual-report-congress.pdf> on 15 April 2021

¹⁷⁵ Retrieved from <https://www.uspis.gov/> on 15 April 2021

information technology assets.”¹⁷⁶ In order to safeguard the integrity, confidentiality, and availability of Postal Service information and protect the interests of its personnel, business partners, and the public, the USPS must observe the policies provided in the handbook. The information security handbook is drafted to take into consideration protection of information as federal laws, regulations, directives, law enforcement and judicial processes, and industry requirements.¹⁷⁷

5.4.13.6 The handbook provides policy on:

- a. The physical and environment security including administrative security controls designed to reduce the risk of physical failure of infrastructure components, damage from natural or fabricated environmental hazards, and use by unauthorised personnel;
- b. personnel security – provides for the appropriate level of personnel clearance to minimise risk to postal service information resources; and
- c. acceptable use - provides for ethical and lawful manner of postal information resources usage.¹⁷⁸

Question 33: Should the Authority require conveyors to give consumer notices explaining how personal data will be used?

5.4.14 Contraventions and Penalties

5.4.14.1 The Postal Service Regulations make provisions for the safe transportation of hazardous material and dangerous goods in the mail and no person may mail material that has been declared nonmailable by statute or postal service regulation to be nonmailable.¹⁷⁹

¹⁷⁶ Retrieved from <https://about.usps.com/handbooks/as805.pdf> on 05 August 2021

¹⁷⁷ Retrieved from <https://about.usps.com/handbooks/as805.pdf> on 05 August 2021

¹⁷⁸ Retrieved from <https://about.usps.com/handbooks/as805.pdf> on 05 August 2021

¹⁷⁹ Retrieved from [eCFR :: 39 CFR Chapter III -- Postal Regulatory Commission](https://www.ecfr.gov/current/title-39-chapter-III) on 15 August 2022

5.4.14.2 According to the 39 U.S. Code 3018 on Hazardous material, a person who knowingly violates such, shall be liable for a civil penalty of at least USD250 (R2 960,23), but not more than USD100,000 (R1,479,315), for each violation; the costs of any clean-up associated with each violation; and damages.¹⁸⁰

5.4.14.3 The OIG reported different cases of mail theft or redirections. After investigations, the culprits were removed from the postal operations and put in jail. This action is supported by the 18 U.S. Code 1708, which declares mail theft a punishable offense with the penalty of a fine or imprisonment.¹⁸¹ The OIG is empowered by the Inspector General Act of 1978, as amended to have unrestricted access to all Postal Service operations, programs, records, and documents, whether in custody of the Postal Service or available by law, contract, or regulation.¹⁸²

5.5 UNITED KINGDOM (UK)

5.5.1 The United Kingdom ("UK") is among the most developed nations with a GDP of \$2.88 trillion in 2021. The island nation has a reported total population of 66,836,327.¹⁸³

5.5.2 The UK postal services are regulated by the Office of Communication ("OFCOM") as legislated in the Postal Services Act of 2011("PSA 2011").¹⁸⁴ The UK Postal market is liberalised, with The Royal Mail, the designated postal operator, mandated to offer universal postal service.

¹⁸⁰ Retrieved from <https://www.law.cornell.edu/uscode/text/39/3018> on 12 August 2021

¹⁸¹ Retrieved from <https://www.law.cornell.edu/uscode/text/18/1708> on 12 August 2021

¹⁸² Retrieved from <https://www.law.cornell.edu/uscode/text/18/1708> on 12 August 2021

¹⁸³ Retrieved from [United Kingdom : Development news, research, data | World Bank](#) on July 2022

¹⁸⁴ Retrieved from [THE FUTURE OF THE UNIVERSAL POSTAL SERVICE IN THE UK Cm 7560 \(publishing.service.gov.uk\)](#) on 22 July 2022

5.5.3 Definitions

5.5.4 UK does not have a definition of the terms mail conveyance and postal article but define key terms used in mail conveyance within the postal services sector. The defined terms include, among others, postal services and types of postal operators. The terms are defined in the following manner:

“Postal services” means

(a) the service of conveying postal packets from one place to another by post,

(b) the incidental services of receiving, collecting, sorting and delivering postal packets, and

(c) any other service which relates to, and is provided in conjunction with, any service within paragraph (a) or (b).

5.5.5 According to Section 28 of the Postal Services Act 2011, *“persons may provide postal services without the need for any licence or authorisation, but the provision of those services by postal operators may be subject to regulatory conditions that OFCOM may impose on them”.*

5.5.6 The postal Services Act defines postal operator as: “a person who provides—
(a) the service of conveying postal packets from one place to another by post, or

(b) any of the incidental services of receiving, collecting, sorting and delivering postal packets.

5.5.7 The UK market offers several types of operators as defined below:

“relevant postal operator” means a postal operator that provides a relevant postal service;

“relevant postal service” means a relevant letters postal service or an untracked DUSP parcel service;

“Universal service provider”: Royal Mail Company

“access operator” means a postal operator that is party to a USP Access Agreement with the universal service provider;

“express and secured service” a service involving the conveyance of postal packets and any incidental services of collecting, sorting and delivering those postal packets which have at least one of the following features: i. a guarantee for delivery by a certain time or date; ii. a facility enabling the sender and the recipient to monitor the progress of a postal packet through the postal operator’s network, including confirmation of delivery;

“intermediary postal operator” means an access operator or any other postal operator that hands over postal packets to another postal operator (including but not limited to the universal service provider) for subsequent conveyance and delivery to the intended recipients of the postal packets

“an access operator or any other postal operator that hands over postal packets to another postal operator (including but not limited to the universal service provider) for subsequent conveyance and delivery to the intended recipients of the postal packets”¹⁸⁵

“Post Office company” means a company that—

(a) is engaged in the provision of post offices,

(b) is or has at any time been—

(i) a subsidiary of the original holding company, or

¹⁸⁵ Retrieved from <https://www.OFCOM.org.uk/postal-services/information-for-the-postal-industry/conditions> on 12 August 2021

(ii) in the same group as a company that is or (as the case may be) was at that time designated under this section, and

(c) is designated for the purposes of this subsection by order made by the Secretary of State.”

5.5.8 Scope

5.5.8.1 The PSA 2011 requires all postal operators to take all reasonable steps to prevent interference with the mail and makes interference with the mail a criminal offence, punishable by fines and/or imprisonment.

5.5.8.2 These essential conditions apply to all relevant postal operators in the UK: Universal service provider, access operator¹⁸⁶, express and secured service¹⁸⁷ and or intermediary postal operator¹⁸⁸ as defined by the Postal Services Act, 2011.

5.5.8.3 Further, Section 51 (1) of the Postal Services Act, empowers OFCOM to impose consumer protection condition on

(a) every postal operator, or

(b) every postal operator of a specified description.¹⁸⁹

¹⁸⁶ Retrieved from https://www.OFCOM.org.uk/data/assets/pdf_file/0021/105258/essential-condition-1.pdf on 24 April 2021

¹⁸⁷ Retrieved from https://www.OFCOM.org.uk/data/assets/pdf_file/0021/105258/essential-condition-1.pdf on 24 April 2021

¹⁸⁸ retrieved from https://www.OFCOM.org.uk/data/assets/pdf_file/0021/105258/essential-condition-1.pdf on 24 April 2021

¹⁸⁹ Retrieved from <https://www.legislation.gov.uk/ukpga/2011/5/section/51> on 12 August 2022

5.5.9 Duties and Powers

- 5.5.9.1 Postal operators are required, through the essential conditions imposed by OFCOM as mandated by Section 49 of the PSA 2011, to take reasonable steps to minimise the risk of the loss, theft, damage or interference of post by implementing and adhering to appropriate policies and procedures.¹⁹⁰
- 5.5.9.2 The consumer protection condition may require every postal operator or every postal operator of specific description to do one or more of the following:
- a. assume liability in respect of specified loss of or damage to certain postal packets;
 - b. establish and maintain procedures, standards and policies with respect to consumer protection matters, and
 - c. make payments relating to qualifying consumer expenses of Citizens Advice and Citizens Advice Scotland.¹⁹¹

5.5.10 Legal possession and ownership of mail items

- 5.5.10.1 The PSA 2011 does not make provisions of legal ownership of mail that is inserted into Royal mail. Postal Services Act, 2011 provides that OFCOM *may impose a consumer protection condition on (a) every postal operator, to assume specified liability in respect of specified loss of or damage to specified postal packets, (b) to establish and maintain procedures, standards and policies with respect to consumer protection matters,*¹⁹²

¹⁹⁰ Retrieved from <https://www.OFCOM.org.uk/postal-services/information-for-the-postal-industry/conditions> on 23 April 2021

¹⁹¹ Retrieved from <https://www.OFCOM.org.uk/postal-services/information-for-the-postal-industry/conditions> on 12 August 2022

¹⁹² Retrieved from [Postal Services Act 2011 \(legislation.gov.uk\)](https://www.legislation.gov.uk/ukpga/2011/12/section/49) on 10 August 2022

5.5.10.2 Royal Mail retail compensation policy provides for the following postal items (1st and 2nd class stamped, metered and VAT exempt account mail, including items sent using online postage etc.) to be compensated upon proof of loss by the post office.¹⁹³

5.5.10.3 The compensation policy provides procedure for customers to claim for loss items. Procedure sets out that: claims for loss must be submitted within 80 calendar days of the date of posting. Claim can be made by both the sender and the recipient, however only one will be compensated. The outcome of the claim will be pronounced by Royal Mail within 30 days of receiving the claim.

5.5.10.4 The claim must also include evidence of having posted the item with Royal mail in order to be processed. Evidence includes, names of sender, receiver, addresses, product of royal mail used, place and date of posting, and description of the mail item posted. For lost or damaged beyond repair items, Royal Mail compensates the actual amount the items costs subject to condition of age and depreciation. For a damaged item, Royal mail compensate only cost of repair and no additional payments for the reduced value of the repaired item.¹⁹⁴

5.5.11 Mail safety and security

5.5.11.1 Essential conditions on security of mail, published by OFCOM imposes an obligation for relevant postal operators to "establish, maintain and adhere to policies and procedures for ensuring the secure conveyance, receipt, collection, sortation, delivery or other handling of relevant postal packets, which shall in particular relate to:

- a. the security of relevant premises;

¹⁹³ Retrieved from <https://www.OFCOM.org.uk/postal-services/information-for-the-postal-industry/conditions> On 23 April 2022

¹⁹⁴ Retrieved from <https://www.royalmail.com/retail-compensation-policy-loss> on 13 August 2021

- b. the use of vehicles and equipment in the collection, conveyance or delivery of relevant postal packets; and
- c. ensuring appropriate processes are followed by relevant employees, and any other permanent, temporary, casual or part-time employees or workers (including those under a contract for service) who are reasonably likely to have access to relevant postal packets in the course of their work, in order to safeguard the security of relevant postal packets".¹⁹⁵

5.5.11.2 Further, the essential conditions impose an obligation to relevant postal operators to implement and adhere to appropriate policies and procedures which includes addressing scale of postal services and activities an operator can carry out; recruitment of relevant employees, training of such employees and disciplinary procedures.¹⁹⁶

5.5.12 Dangerous and prohibited goods

5.5.12.1 In the UK, certain dangerous goods are allowed to be conveyed through end-to-end postal operators in small quantities without applying the full regulations on Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009 (as amended) (CDG 2009).¹⁹⁷ The conditions imposed upon postal operators to carry out such include amongst others:

- a. "written company Dangerous Goods Policy setting out the organisation's minimum standards and processes to achieve compliance and training of personnel to be handling such.
- b. Raise awareness concerning dangerous goods and the terms of their acceptance with its external customers

¹⁹⁵ Retrieved from https://www.OFCOM.org.uk/data/assets/pdf_file/0021/105258/essential-condition-1.pdf on 24 April 2021

¹⁹⁶ Retrieved from https://www.OFCOM.org.uk/data/assets/pdf_file/0021/105258/essential-condition-1.pdf on 24 April 2021

¹⁹⁷ Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876870/authorisation-284.pdf on 23 April 2021

- c. Raise awareness of the dangerous goods policy and its application with internal staff.
 - d. Train personnel implementing the dangerous goods policy, commensurate with their responsibilities.
 - e. keep a current record of all dangerous goods training given to individual personnel.”¹⁹⁸
- 5.5.12.2 The conveyance of dangerous goods in post, including (but not limited to) alcohol and perfume,¹⁹⁹ is regulated as set out by the UPU rules under article 19 of the UPU convention manual. Royal Mail Group publishes on their website goods to be carried and conditions of carriage²⁰⁰.

Question 34: In addition to publishing the list, should the Authority require conveyors to raise awareness on dangerous and prohibited goods?

5.5.13 Monitoring and Reporting

- 5.5.13.1 To ensure compliance and usefulness of the essential condition, postal operators are obliged to monitor and review relevant policies and procedures.
- 5.5.13.2 They are also required to record and submit to OFCOM and the Consumer Advocacy Bodies reports, in a manner provided in the essential condition, within three months of the end of the relevant period regarding all incidents of loss or theft of, damage to, or interference with relevant postal packets.

¹⁹⁸ Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876870/authorisation-284.pdf on 23 April 2021

¹⁹⁹ Retrieved from <https://www.gov.uk/government/publications/notice-143-a-guide-for-international-post-users/notice-143-a-guide-for-international-post-users?step-by-step-nav=1faad9b3-e5ef-47f6-a3ba-4715e7e4f263> on 23 April 2021

²⁰⁰ Retrieved from https://personal.help.royalmail.com/app/answers/detail/a_id/96/~/prohibited-and-restricted-items---advice-for-personal-customers on 23 April 2021

5.5.13.3 Further, relevant postal operators are required to manage and ensure compliance by their franchisees, agents and sub-contractors to these essential conditions.

5.5.14 Cybersecurity

5.5.14.1 Data privacy and security law in the UK is regulated by the General Data Protection regulations (GDPR) 2018, which controls how personal information is collected and used by organisations, businesses or the government. Data protection principles to be followed include, obtaining consent for collection, fair and transparent usage of data; for specified, explicit purposes; limited to only what is necessary; and kept up to date, for a period of time.²⁰¹

5.5.14.2 Royal mail has also been targeted by cyberattacks. One such popular attack reported is a message sent from Royal Mail with a malicious link to release a postal item, this has led to people being defrauded of their money.²⁰²

5.5.14.3 In terms of data protection, Royal Mail has put in place numerous data policies, procedures and processes in order to safeguard personal information of all its stakeholders (customers and employees).²⁰³

5.5.14.4 Royal mail data protection policy²⁰⁴ sets out privacy principles in accordance with the data protection laws and principles of the country (UK GDPR) which include collecting data that is relevant and used it for the sole purpose it was collected to, processed within the ambit of the law and report data breaches incidents etc.

²⁰¹ Retrieved from <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted/data.htm> on 5 August 2021

²⁰² Retrieved from <https://www.express.co.uk/life-style/life/1446423/royal-mail-scam-warning-uk-postage-dispatch-fee-latest-news> on 5 August 2021

²⁰³ Retrieved from <https://www.royalmail.com/gdpr> on 5 August 2021

²⁰⁴ Retrieved from <https://www.royalmail.com/gdpr> on 5 August 2021

- 5.5.14.5 Royal Mail has put in place internal data retention policies which cover the requirements for data retention and secure disposal/destruction of information waste.²⁰⁵
- 5.5.14.6 In addition to the data privacy and protection policy, Royal mail developed Information Security positioning statement²⁰⁶ which aims to assure stakeholders and customers that data and information systems are protected from relevant security threats. Practical solutions provided in the document include the locking of employee laptops by end point security solutions including malware protection, drive encryption, and centralised monitoring, with configuration policies globally enforced from a central IT authority.²⁰⁷
- 5.5.14.7 Moreover, employees and contractors are vetted pre-employment and confidentiality clauses are included in their contracts. Abuse or misuse of information or technical assets can lead to dismissal of employees or termination of services from contractor.²⁰⁸

5.5.15 Contraventions and Penalties

- 5.5.15.1 The Postal Services Act, 2011 requires OFCOM to notify any person if OFCOM determine that there are reasonable grounds to believe that the person is contravening, or has contravened, a regulatory requirement. The Postal Services Act, 2011 empowers OFCOM to impose a penalty on a person if the person has been in contravention of a requirement specified in the notification, and the fee may also be determined by OFCOM.²⁰⁹

²⁰⁵ Retrieved from <https://www.royalmail.com/gdpr> on 24 April 2021

²⁰⁶ Retrieved from <https://www.royalmail.com/gdpr> on 06 August 2021

²⁰⁷ Retrieved from <https://www.royalmail.com/gdpr> on 06 August 2021

²⁰⁸ Retrieved from <https://www.royalmail.com/sites/royalmail.com/files/2021-06/RMG-InfoSec-Positioning-statement.pdf> on 06 August 2021

²⁰⁹ Retrieved from <https://www.legislation.gov.uk/ukpga/2011/5/schedule/7> on 12 August 2021

5.5.15.2 Under the Postal Services Act, 2011, Royal Mail is charged with the duty to protect the security of mail therefore, minimising the risk of its exposure to loss, theft, damage, or interference. In this regard, OFCOM has published Mail Integrity Code of Practice (MICOP) with essential conditions to be complied to by postal operators.

5.5.15.3 Furthermore, under the Postal Services Act, 2011, person or personnel of the post office is considered to have committed offence if the person interferes with mail by “intentionally delaying or opening a postal packet in the course of its transmission by post, or intentionally opens a mail-bag.” That person is upon conviction, liable to a fine not exceeding the statutory maximum or to imprisonment for a term not exceeding six months or to both.²¹⁰

5.5.15.4 Another contravention is of sending prohibited articles by post; if such a person is convicted, they will be liable to a fine not exceeding the statutory maximum, or to imprisonment for a term not exceeding twelve months or to both.²¹¹

5.5.15.5 Furthermore, no person is to affixing advertisements on letter boxes, otherwise, such person will, upon conviction, be liable to a fine as set in the standard scale level 3.

5.5.15.6 And it is prohibited to make misleading descriptions on the post office, if such offense is committed, then, upon conviction such person shall be liable to a fine not exceeding level 3 on the standard scale.²¹²

²¹⁰ Retrieved from <https://www.legislation.gov.uk/ukpga/2000/26/part/V/crossheading/offences-of-interfering-with-the-mail> on 12 August 2021

²¹¹ Retrieved from <https://www.legislation.gov.uk/ukpga/2000/26/part/V/crossheading/offences-of-interfering-with-the-mail> on 12 August 2021

²¹² Retrieved from <https://www.legislation.gov.uk/ukpga/2000/26/part/V/crossheading/offences-of-interfering-with-the-mail> on 12 August 2021

5.6 ZIMBABWE

5.6.1 Zimbabwe is a developing country with an economy mostly reliant on agriculture sector and export of minerals. The Zimbabwe GDP is estimated to have grown by 5.8% in 2021. Zimbabwe's total population is estimated to amount to 15,092,171.²¹³

5.6.2 Zimbabwe postal services are regulated by Postal and Telecommunication Regulatory Authority of Zimbabwe ("POTRAZ") as legislated by the Postal and Telecommunications Act, of 2000 (Act of 2000)²¹⁴. Zimbabwe Post (Zimpost) is a designated postal operator in Zimbabwe responsible for providing universal postal services.

5.6.3 Definitions

5.6.4 The Act of 2000 does not have a definition of the term mail conveyance. Terms such as mail, and postal article, amongst others, are defined in the following manner:

"mail means any article which is deposited in a post box for collection and conveyance by post or which is being conveyed by post;

"postal service" means a service comprising—

(a) the conveyance for reward of postal articles from one place to another, whether by land, sea or air; and

(b) the performance of all services incidental to the receiving, collecting, sending, despatching and delivering of postal articles; and

²¹³ Retrieved from [Zimbabwe: Development news, research, data | World Bank](#) on 07 August 2022

²¹⁴ Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_Act.pdf on 18 March 2022

(c) the issuance of money orders and postal orders; and includes a commercial courier service, but does not include—

(i) the provision of postage stamps, unless expressly authorised by the terms of a postal licence; or

(ii) the provision of an electronic mail service, except in accordance with a telecommunication licence;

“postal article” includes any letter, postcard, printed paper, small packet, newspaper, literature for the blind, parcel or other article whatsoever in the course of transmission by post.

“post” means any system for the collection, dispatch, conveyance, handling and delivery of postal articles by or through a postal licensee;”²¹⁵

5.6.5 Scope

5.6.5.1 Zimbabwe does not prescribe specific regulations in terms of mail conveyance. Regulation of mail conveyance is provided for in the Postal and Telecommunications (Postal Services) Regulations, 2001. The scope of the Postal and Telecommunications (Postal Services) Regulations, 2001 apply to all postal licensees. The postal licensees include a postal service (general), a commercial international courier service, a commercial domestic courier service licensee.²¹⁶

5.6.5.2 Part III of the Postal and Telecommunications (Postal Services) Regulations, 2001 provides clauses on transmission of postal articles

²¹⁵ Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_Act.pdf on 18 March 2022

²¹⁶ Retrieved from https://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_238_OF_2001.pdf on 10 August 2022

including packing of postal articles; transmission of restricted articles, method of addressing parcels and methods of packing parcels.²¹⁷

5.6.6 Powers and Duties

- 5.6.6.1 Zimpost is licenced under the Act of 2000 to provide universal postal service as licensed, erect, maintain and use posting boxes and postage label vending machines in any public road, street or highway or in any other public place, and may remove any such posting box or postage label vending machine erected by it and provide for philatelic services.²¹⁸
- 5.6.6.2 Zimpost may decline delivery of postal article where postage is not paid, may demand payment of postage from customer and/or dispose postal article that are not deliverable.²¹⁹
- 5.6.6.3 Zimpost is empowered to open and examine the postal article for the purpose of determining from its contents the identity and address of the addressee or sender; if, on an examination the suspicion that gave rise to its examination is substantiated, the postal article may be detained with the intention to destroy or dealt with a manner prescribed.²²⁰
- 5.6.6.4 Secondary to the Act of 2000 is the Postal and Telecommunications (Postal Services) Regulations, 2001 which provides for the licensing and operations of the postal operator. The Postal and Telecommunications (Postal Services) Regulations, 2001 stipulates that the postal licence may provide terms and guidelines, in accordance with the UPU Constitution and

²¹⁷ Retrieved from https://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_238_OF_2001.pdf on 10 August 2022

²¹⁸ Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_Act.pdf on 18 March 2022

²¹⁹ Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_Act.pdf on 18 March 2022

²²⁰ Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_Act.pdf on 18 March 2022

Convention and other international agreements on postal services, to be adopted in the operation of the service.²²¹

5.6.7 Legal Ownership and Possession of Mail

5.6.7.1 The Act of 2000 does not clearly state the definition of when is the postal article legally in custody of the postal licensee however deems mail to be delivered to the person whom the postal article is addressed to when it is dropped:

"(a) at the address specified thereon; or

(b) according to the usual manner of delivery to the person to whom the postal article is addressed, at his house or office or to his servant or agent or another person considered by the postal licensee to be authorized to receive the postal article; or

*(c) into a private box or private bag leased or used by the person to whom the postal article is addressed or, with the consent of the lessee or user thereof and of the person to whom the postal article is addressed, into any other private box or private bag."*²²²

5.6.7.2 Further provide that "a postal licensee shall not be liable in respect of any injury, loss or damage suffered by any person by reason of—

(a) any loss, mis delivery or delay of or damage to any postal article in the course of transmission by post; or

(b) any failure to provide or delay in providing any postal service or any equipment associated therewith or service ancillary thereto; or

(c) any failure, interruption, suspension or restriction of any postal service or service ancillary thereto or delay of, or fault in, any communication by post; or

²²¹ Retrieved from https://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_238_OF_2001.pdf on 10 August 2022

²²² Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_238_OF_2001.pdf on 18 March 2022

(d) any loss of secrecy in communication arising from the use of any postal service; or

(e) any wrong payment or delay in payment in connection with any remittance of money through the post or any other irregularity in the document used in connection with the remittance.”²²³

5.6.7.3 The Postal and Telecommunications (Postal Services) Regulations, 2001 further provides for the insurance and or registration of certain postal articles against loss (liquids, perishable articles, fragile articles such as glassware) or damage, and makes other articles insurance compulsory (such as jewellery, precious stones etc.). The maximum amount of insurance as prescribed by the POTRAZ or that set in the country of the origin sender, whichever one that is less.

5.6.7.4 In the event of the “loss of or damage to any article enclosed in or forming part of a parcel or an insured postal article, or the loss of any registered postal article while in the custody of a postal licensee, the licensee may pay an indemnity in accordance with the provisions of the Constitution of the UPU or any international agreement to which Zimbabwe is a party.”²²⁴

5.6.7.5 According to the Postal and Telecommunications (Postal Services) Regulations, 2001, however if the damage to the article was a result of non-observance of the conditions for conveyance, then the sender of a postal article shall be liable, to the same extent to which the postal licensee would be liable as set above.²²⁵

5.6.7.6 The Postal and Telecommunications (Postal Services) Regulations, 2001, clearly stipulates that compensation for damage to or loss of postal article

²²³ Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_238_OF_2001.pdf on 18 March 2022

²²⁴ Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_238_OF_2001.pdf on 18 March 2022

²²⁵ Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_238_OF_2001.pdf on 18 March 2022

shall be given to the sender of the postal article in respect of which compensation is claimed.²²⁶

5.6.8 Prohibited and Dangerous goods

5.6.8.1 Zimbabwe conforms to the UPU rules of conveyance of dangerous goods by post. Clause 17 of the Postal and Telecommunications (Postal Services) Regulations, 2001, provides that:

"(1) A person authorized under any law in force in Zimbabwe to import opium, morphine, cocaine or any narcotic may, subject to the provisions of that law, send such articles by post.

5.6.8.2 And further prescribes a manner in which restricted articles can be transmitted by posts on condition that:

"(a) it is sent in the interest of public health;

(b) it is sent at the rate of postage prescribed for the transmission of letters; and

(c) liquids, oils and substances which easily liquefy are enclosed in a receptacle hermetically sealed and such receptacle is placed in a special box of metal, strong wood or strong corrugated cardboard containing sawdust, cotton or spongy material in sufficient quantity to absorb the liquid in the event of the breakage of the receptacle, and the lid of the box is fixed in such a manner that it cannot easily become detached."²²⁷

5.6.9 Cybersecurity

5.6.9.1 Zimpost is looking into taking advantage of the digital developments with the launch of an e-commerce Mall that has become popular within

²²⁶ Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_238_OF_2001.pdf on 18 March 2022

²²⁷ Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_Act.pdf on 18 March 2022

Zimbabwe. Zimabwemall is based on an inclusive partnership business model with high security standards.²²⁸

- 5.6.9.2 The platform has allowed local businesses access to domestic and international markets without making additional investment in technology. This platform using the secure internet infrastructure of Zimpost, based on the top-level domain [.POST](#), sponsored by the UPU. The domain charges no rental fees for sellers. UPU's. POST domain, provides a robust cybersecurity shield that helps prevent cyberattacks and protect businesses.²²⁹
- 5.6.9.3 In 2021, Zimpost launched a PostMoney Centre and digital money order service, which enables users to send multi-currencies, with delivery notifications within a day provided over Zimbabwe mobile networks.
- 5.6.9.4 Zimbabwe is a signatory to the UPU and CRASA. The country has been working towards harmonising its cybersecurity laws to fight cybercrime. The DATA Protection Act of 2021, consolidates cyber related offenses and provide for data protection to increase data protection in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects.²³⁰
- 5.6.9.5 The DATA Protection Act of 2021 is applicable "(a) to the processing of data carried out in the context of the effective and actual activities of any data controller; (b) to the processing and storage of data by a controller who is not permanently established in Zimbabwe, if the means used, whether electronic or otherwise is located in Zimbabwe, and such processing and

²²⁸ Retrieved from <https://etradeforall.org/news/driving-digital-economy-in-africa-through-inclusive-and-secure-e-commerce/> on 18 March 2022

²²⁹ Retrieved from <https://etradeforall.org/news/driving-digital-economy-in-africa-through-inclusive-and-secure-e-commerce/> on 18 March 2022

²³⁰ Retrieved from http://veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf on 18 March 2022

*storage is not for the purposes of the mere transit of data through Zimbabwe.*²³¹

- 5.6.9.6 The Data Protection Act 2021 establishes POTRAZ as the Cyber Security Centre and the Data Protection Authority. POTRAZ shall provide guidelines and approve codes of conduct and ethics governing the rules of conduct to be observed by data controllers and categories of data controllers. POTRAZ shall also establish rules giving the authorisation for and governing the whistleblowing system.
- 5.6.9.7 The Minister responsible for information and communications technologies may in consultation with POTRAZ, make regulations providing for all matters required or permitted to be prescribed or which, in his or her opinion, are necessary or convenient to be prescribed for carrying out or giving effect to this the Data Protection Act of 2021.²³²
- 5.6.9.8 Furthermore, the Data Protection Act of 2021 provides for general rules on the processing of data (which is fair, lawful and specific purpose); sets out standards and strict obligations on collection, processing and usage of data to ensure transparency and accountability.²³³
- 5.6.9.9 The Data Protection Act of 2021 provides for the investigation and collection of evidence for cybercrime and data breaches, allowing the admissibility of electronic evidence by courts as part of measures to ensure a safer cyberspace for citizens.

²³¹ Retrieved from http://veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf on 18 March 2022

²³² Retrieved from http://veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf on 18 March 2022

²³³ Retrieved from http://veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf on 18 March 2022

5.6.10 Contraventions and Penalties

5.6.10.1 The Act of 2000 provides for several offences in relation to mail conveyance and the penalties. The fines imposed are set according to levels of criminal law standard fine scales. The sections are provided below:

5.6.10.2 *“Section (80) provides for the offence of forgery of stamps and money orders, etc. and if one is found guilty of this offence, shall be liable to a fine not exceeding level eleven or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.*

5.6.10.3 *Section (82) provides for offences in relation to negligence (detains, delays, misdeliver or omits dispatch), misconduct (including unlawfully divulging contents) and endangering the safety of any mail or postal article. This is an offence and liable to a fine not exceeding level six or to imprisonment for a period not exceeding one year or to both such fine and such imprisonment.*

5.6.10.4 *Theft of and tampering with mail is also an offence and liable to a fine not exceeding level eleven or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.*

5.6.10.5 *Section (84) provides for an offence of sending restricted and prohibited postal articles and transmission of dangerous substances punishable by a fine not exceeding level six or imprisonment for a period not exceeding one year or both such fine and such imprisonment.*²³⁴

5.6.10.6 Sending any of the Dangerous Drugs specified to be prohibited by the Dangerous Drugs Act is an offence punishable by a fine not exceeding level

²³⁴ Retrieved from http://www.potraz.gov.zw/wp-content/uploads/2015/04/Postal_Act.pdf on 18 March 2022

eleven or imprisonment for a period not exceeding seven years or both such fine and such imprisonment.

6 LESSONS FOR MAIL CONVEYANCE REGULATION IN SOUTH AFRICA

6.1 There are various lessons that can be learnt from the countries benchmarked above. Some lessons can help enhance the quality of the Regulations. While others can help improve enforcement of the Regulations. There are, however, limitations to what can be deemed as lessons that can be adopted and the extent to which they can be implemented as they are mostly moulded by their respective legislative frameworks.

6.2 Regulation of Mail Conveyance

6.2.1 The Authority is empowered to make the Regulations under section 61 (d) of the PSA, wherein it has the power to make regulations for the conveyance of postal articles, general powers and duties of conveyors, legal possession or ownership of postal articles.

6.2.2 Benchmarking illustrates that different various countries regulate the conveyance of mail differently. Tanzania and Zimbabwe have general postal regulations that incorporate mail conveyance. Whereas the UK, Malaysia and the USA do not have specific regulations that incorporate mail conveyance.

6.2.3 The UK has essential conditions that seek to take reasonable steps to minimise the risk of the loss, theft, damage or interference of post by implementing and adhering to appropriate policies and procedures. In Malaysia, the regulator has the powers to make rules on all matters pertaining to mail conveyance.

6.2.4 The USA has rules and procedures (information) in the USPS Guide to Mail Centre Security. The rules deal with mail security, risks assessment, prohibited goods, handling and processing mail safely.

6.2.5 Mail conveyance is not left to self-regulation. There are countries that have regulations, standards or rules that permit and/or prohibit certain activities and also protect consumers in the conveyance of mail. While other countries dedicate clauses in the general postal regulations to the conveyance of mail.

6.2.6 Definitions

6.2.6.1 Mail conveyance is not generally defined as a term or as a postal services business activity. Different countries have defined mail and other postal services sector terms used in relation to mail conveyance. The most commonly defined term is mail, which is defined in various ways but with a similar meaning. Some of the terms defined include, amongst others, postal article, post and postal network.

6.2.6.2 Malaysia is the only country, among those benchmarked, that defines mail conveyance as "*the mode used to transmit postal articles*". This definition is dependent on the definition of postal article and transmission of postal article. Both these terms are also defined, and they give context and holistic meaning to mail conveyance.

6.2.6.3 As seen in benchmarking, it is imperative to define mail conveyance, or the key terms associated with or used in mail conveyance activities, and not leave the term as a jargon mostly used and understood by those in the postal services sector. The definition of mail conveyance or associated terms must cater to the general public.

6.2.7 Scope

6.2.7.1 The Regulations apply to all conveyors of mail falling under the ambit of Schedule 1 and 2 of the PSA and whose business includes to carry, transfer or deliver mail from the sender to the intended destination.

- 6.2.7.2 Similarly, regulations, standards and rules, that pertain to mail conveyance, in benchmarked countries are applicable to all licensees and operators involved in the business of conveying mail, except in the USA. The USPS Guide to Mail Centre Security scope is limited to the USPS.
- 6.2.7.3 Most benchmarked countries deem it important to regulate the movement of mail by all licensees and operators. Regulations and rules create transparent sector practices, provide postal services consumers with necessary protection and ensures safety and security of mail.

6.2.8 Duties and Powers of the Conveyor

- 6.2.8.1 Primary duties and powers of the conveyor/licensee is of the conveying of mail from the sender to the addressee. Provisions for these may be provided for in the national Postal Services Act and further echoed in the terms and conditions of the operator's license. The conveyor/licensee must comply with the conditions specified for the provision of postal services.
- 6.2.8.2 Most benchmarked countries do not have specific set of regulations on conveyance of mail that specifies duties and powers for conveyance. The duties and powers of the conveyor are stipulated in the Postal Services Act and further laid out in various pieces of Regulations.
- 6.2.8.3 Drawing from the benchmark, general duties and powers for conveyors/licensees may include but not limited to performing duties and obligations as a universal or no-universal service provider which entails frequently through a reliable, safe and secure system, collect, transmit and deliver any postal article. Further, countries put in place policies that focus on consumer protection matters. The emphasis is on who assumes liability in respect of specified loss of or damage to certain postal articles and pay compensation for such in line with regulations laid out.

6.2.9 Ownership and legal possession of postal items

- 6.2.9.1 The Regulations deems possession of mail to the conveyor the moment that mail is handed to the conveyor or agent and possession of mail passes to the addressee upon delivery of mail. The requirement for legal possession of mail can absolve the conveyor the liability of damage, loss and theft of mail as is the case in Malaysia.
- 6.2.9.2 The UPU assigns ownership of mail to the sender until it is delivered to the rightful owner. This provision is also applicable in Malaysia, Tanzania, the USA, the UK and Zimbabwe. All these countries consider mail to be delivered when it is handed or delivered to addressee or deposited in a post office locked bag or letter box or any other receptacle or device provided for the receipt of postal article of the addressee.
- 6.2.9.3 In terms of liability of loss or damage and compensation of postal articles, benchmarked countries handle liability and compensation in similar ways. Compensation is paid according to the set regulations or conditions. Wherein the sender is found to have contravened the conditions or regulations, the conveyor is exempt from liability.
- 6.2.9.4 In some cases, like Malaysia, legislation exempt Pos Malaysia from liability of postal items unless it is proven that the conveyor has maliciously or negligently or intentionally cause the loss, mis-delivery, delay or damage.
- 6.2.9.5 In the UK, claims for lost or damaged postal items can be made by both the sender and the recipient, however only one will be compensated.

6.2.10 Mail safety and security

- 6.2.10.1 Mail safety and security is at the centre of the mail conveyance business activities. In the Regulations, conveyors are obliged to adopt and put in

place, strict access control measures to where mail is kept and provides examples of measures to put in place in line with the UPU security measures.

6.2.10.2 All benchmarked countries have extensive and similar mail safety and security requirement measures in place. They have provisions and obligations for the conveyors/licensees to put in place safety measures to protect and improve mail security and combat postal crimes.

6.2.10.3 The focus is ensuring mail integrity through specific and reasonable security measures to protect the postal network facilities, to prioritise recruitment of relevant employees, the training of such employees and the use of secure vehicles in conveyance of mail.

6.2.11 Dangerous and prohibited items

6.2.11.1 The benchmark shows that countries are aligned to the UPU rules on dealing with prohibited and dangerous goods in the postal network. Licensees and conveyors reserve the right to amend the list of prohibited and dangerous good as and when a need arises. In addition, benchmark shows that there is a recognition of the rapid market changes, growth of e-commerce, and the growing consumer needs that necessitate flexibility in the lists of dangerous and/or prohibited items in the postal network.

6.2.11.2 The countries also recognise the shift in business platform to digital and therefore do not dictate to the conveyors a place to publish the list and only put an obligation for conveyors keep the list for the benefit of consumers. However, some countries like Tanzania do not put an obligation for the licensees to publish the list for the benefit of consumers. Rather the obligation is on the postal licensee to inform and handover to the TCRA any goods suspected to be in contravention of the EPOCA Act or country laws of dangerous goods.

6.2.11.3 Furthermore, benchmarked countries allow some prohibited and dangerous good to be conveyed under strict conditions as stipulated by the UPU. The conditions extend the liability of damage to postal infrastructure and returning mail to the sender.

6.2.12 Cybersecurity

6.2.12.1 Benchmark shows that countries do not have specific legislations addressing cybersecurity in the postal services sector, but they have various pieces of legislations dealing with different aspects of cybercrimes. licensees and conveyors are obliged to adopt and implement national laws meant to prevent and to reduce the incidences of domain hijacking, phishing and spoofing in the postal sector, as they lead to identity theft and fraud.

6.2.12.2 In addition, the benchmark does not indicate any inclusion of clauses in the regulations to oblige different licensees to put in place cybersecurity measures including privacy protection. However, operators are allowed to deal with issues of cybersecurity and privacy protection in line with their country's national legislation.

6.2.13 Contraventions and Penalties

6.2.13.1 The UPU recommends member countries to adopt the necessary measures to prevent, prosecute and punish any person found guilty of their stipulated rules on mail conveyance, security and dangerous and prohibited goods in the postal network. The UPU does not set the floor nor the ceiling on punishment of any of such crimes.

6.2.13.2 The benchmark indicates that every country included in this study has put in place the contraventions and set their penalties in line with their

countries' legal standards. The penalties are set between a fine or imprisonment and can be both for other offenses.

7 CONCLUSION

The Discussion Document is based on information gathered from the desktop research. The extensive research provided from international benchmarking and international guidelines and treaties has been used to aid in the process of public consultation on the conveyance of mail inquiry. The committee will consider every submission from the public to produce a findings document which will assist make determination on the way forward.