UNIVERSAL POSTAL UNION

UPU International Bureau
Weltpoststrasse 4
3015 BERNE
SWITZERLAND

T +41 31 350 31 11
F +41 31 350 31 10
www.upu.int

Contact: Mr Bonseung Ku
T +41 31 350 35
Bonseung.ku@upu.int

To: Designated operators of Union member countries

Berne, 5 December 2023

Reference: 3911(DPRM.PPRE.PRA)1159
Subject: Survey on member countries' regulatory frameworks on data collection and protection

Dear Sir/Madam,

In accordance with the Universal Postal Convention, Union member countries are required to undertake a number of activities associated with essential or mandatory data exchanges. The data exchanged in the course of such activities often includes personal data, such as the names and physical addresses of senders and recipients.

The current regulatory framework regarding the protection of personal data is based on a number of provisions set out in the Convention and its Regulations, as well as in the Postal Payment Services Agreement (PPSA) and the UPU Multilateral Data Sharing Agreement (MDSA) framework. Nevertheless, most provisions of this nature rely heavily on the national legislation of each member country. Moreover, while the MDSA stipulates specific obligations relating to the exchange of personal data, the framework is not mandatory, which means that there are still links in the postal supply chain that may be vulnerable to data breaches and other forms of abuse.

In this context, the 27th UPU Congress decided to conduct a survey and analytical study on data collection and protection policies and regulations in Union member countries.[1] The objective is to understand the current practices of designated operators (DOs) in relation to the protection of personal data. Based on that understanding, the UPU aims to develop regulatory advisory services for DOs with a view to supporting them in developing appropriate frameworks to safeguard the processing and transmission of personal data between them and other DOs and/or other postal sector stakeholders in the context of international postal operations. The results of the survey will also be considered in the Council of Administration's review of the regulatory and policy frameworks governing data collection and protection.

Pursuant to this mandate, we are sending you the attached survey, designed to gather information on UPU member countries' regulatory frameworks with regard to data collection and protection. You are kindly asked to complete the questionnaire in Annex 1 and return it to the International Bureau **by 19 January 2024 at the latest**. The survey questionnaires are also available on the UPU website at www.upu.int/en/members-centre/policies-regulation.

Yours faithfully,

Siva Somasundram
Director of Policy, Regulation and Markets

[1] Abidjan Business Plan work proposal 1.2.13 PPR 1 on treaty obligations for universal service, regulation and postal policy (see strategic output SP 132).

Survey on data collection and protection policies and regulations in the international postal service

Designated operators of UPU member countries are asked to complete and return this questionnaire (without a covering letter) as soon as possible, but **by no later than 19 January 2023**, to the following address:

Mr Bonseung Ku
Policy and Regulatory Advisory Associate Expert
International Bureau
Weltpoststrasse 4
3015 BERNE
SWITZERLAND

The completed survey can also be returned by e-mail to bonseung.ku@upu.int.

Should you have any problems in completing this questionnaire, please contact Mr Bonseung Ku at the International Bureau (+41 31 350 35 24 or bonseung.ku@upu.int).

Please describe your organization type (select one) ❑ Supervisory ministry (responsible for the postal sector) ❑ Regulator (responsible for the postal sector) ❑ Designated operator	
Name of organization	
Full name ❑ Mr ❑ Ms	
Position/title	
Address	
Country	
Tel.	Fax

Questionnaire

Part I – General questions

1 In your national postal operations, what data protection/privacy regulation[1] are you subject to?

- ❑ General Data Protection Regulation (GDPR) (European Union regulation)
- ❑ Swiss Federal Act on Data Protection (FADP)
- ❑ California Consumer Privacy Act (CCPA)
- ❑ Brazilian General Personal Data Protection Law (LGPD)
- ❑ None
- ❑ Other (please specify):

2 Are there postal sector specific regulations[2] on data protection in your country?

- ❑ Yes (please specify):
- ❑ No

3 Are there other *cross-sector* data protection regulations, such as in relation to customs and transport, which are relevant to the postal sector in your country?

- ❑ Yes (please specify):
- ❑ No

4 For what purposes do you collect and exchange personal data[3] with other parties in the operation of international postal services? Please select all applicable options (more than one answer is possible):

- ❑ Operational purposes (collection, processing, tracking/item identification, addressing, delivery, etc.)
- ❑ Customs and security (electronic advance data, ITMATT data, etc.)
- ❑ Quality of service (such as customer feedback and delivery performance)
- ❑ Financial and accounting (such as billing information, payment details)
- ❑ Other (please specify):

[1] Data protection/privacy regulation refers to the rules and standards that govern how personal data is collected, used, stored and shared.
[2] Sector specific regulations are those that apply only to the postal sector and may have different or additional requirements than the overall data protection regulations.
[3] Personal data refers to any information that can be used to identify or relate to a natural person.

The UPU Multilateral Data Sharing Agreement (MDSA), adopted by the POC in April 2021, is a legal instrument created to facilitate the exchange of data necessary for the operation of international postal services and to enable the implementation of such exchanges in accordance with the UPU Acts.

The MDSA incorporates and expands on the substantive provisions of existing and privately established multilateral data sharing arrangements concluded by the designated operators of Union member countries. The goal is to better reflect the relevant data-sharing obligations contained in the Acts of the Union and to establish the relevant conditions for a UPU-managed instrument with global reach.

5 Are you a signatory of the UPU MDSA?

- ❑ Yes
- ❑ No
- ❑ Other (please specify):

Part II – Accountability

6 Do you have a dedicated data protection officer (DPO) or similar person responsible for ensuring compliance with data protection and privacy obligations? (Please select only one answer among the following):

- ❑ We have a dedicated DPO or team who monitors and updates our policies and procedures regularly
- ❑ We rely on external consultants or auditors who review and advise us on our policies and procedures periodically
- ❑ We do not have a formal DPO or team who monitors and updates our policies and procedures regularly
- ❑ Other (please specify):

7 How do you demonstrate accountability for data protection/privacy to your customers and partners? Please select all applicable options (more than one answer is possible):

- ❑ We publish our data privacy policy and notices on our website and via other communication channels
- ❑ We conduct regular data protection impact assessments[4] and audits and report the results thereof to our stakeholders
- ❑ We do not have a specific way of demonstrating our accountability for data privacy
- ❑ Other (please specify):

[4] A data protection impact assessment is a process for identifying and mitigating risks associated with the processing of personal data.

Part III – Information obligations

8 How do you inform data subjects[5] of the means and purposes for which their personal data is being processed[6]? Please select all applicable options (more than one answer is possible):

- ❑ Privacy notice
- ❑ Terms and conditions
- ❑ E-mail
- ❑ Consent forms
- ❑ None
- ❑ Other (please specify):

9 How do you ensure that personal data is processed solely for the purposes for which it was gathered? Please select all applicable options (more than one answer is possible):

- ❑ Regularly review and update privacy policies and consent forms to align with the specific purposes of data collection
- ❑ Provide clear and transparent communication with data subjects regarding the intended use of their personal data and obtain explicit consent for any additional purposes
- ❑ We have no defined method for ensuring that personal data is processed solely for the purposes for which it was gathered
- ❑ Other (please specify):

Part IV – Confidentiality and security of data exchanges

10 How do you prevent unauthorized sharing of confidential information[7]? Please select all applicable options (more than one answer is possible):

- ❑ We provide regular training and awareness programmes on data privacy and confidentiality obligations
- ❑ We have written policies and procedures that specify the roles and responsibilities of data handlers and the consequences of non-compliance
- ❑ We use technical and organizational measures[8] to protect confidential information from unauthorized access, use, modification or disclosure

[5] Data subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity. In other words, a data subject is an end user whose personal data can be collected.

[6] Processing personal data means any operation or set of operations performed on personal data, such as collection, storage, use, disclosure, or deletion.

[7] Unauthorized sharing of confidential information means disclosing or using information that is meant to be restricted to certain individuals or entities.

[8] Technical measures encompass mechanisms such as encryption, access controls to safeguard information and organizational measures involving the implementation of procedures and practices to manage and mitigate risks related to data processing.

- ❑ We monitor and audit the data handling activities and report any breaches or incidents to the relevant authorities and parties
- ❑ Other (please specify):

Concerning questions 11 through 15, the UPU recognizes that you may be using the technologies and services provided by its Postal Technology Centre (PTC), and specifically the International Postal System (IPS) and/or Customs Declaration System (CDS) with, in some cases, software hosting also provided by the PTC (Cloud and .post services). In such cases, part of the answers to the questions below can come from the PTC operations. We kindly ask you, however, to answer these questions and to complement your answers with the measures that you take locally.

11 Do you have an emergency plan[9] and a backup system in place to ensure the continuity of the service and the resumption of activities in case of an unplanned interruption or other emergencies? (Please select only one answer among the following):

- ❑ Yes, we have both an emergency plan and a backup system
- ❑ No, we do not have an emergency plan or a backup system
- ❑ Other (please specify):

12 How do you monitor and report any security breaches[10] related to the personal data exchanged with other parties? (Please select only one answer among the following):

- ❑ We have a dedicated security team or unit that monitors and reports any security breaches
- ❑ We have a security breach response policy or procedure that guides our monitoring and reporting activities
- ❑ We rely on the security features or alerts of our systems or networks to detect and report any security breaches
- ❑ We do not monitor or report any security breaches
- ❑ Other (please specify):

13 Which parties do you notify in the case of a security breach? Please select all applicable options (more than one answer is possible):

- ❑ UPU International Bureau
- ❑ Local data protection authorities
- ❑ Affected data subjects
- ❑ Affected counterparties

[9] An emergency plan is a set of procedures and actions that aim to prevent, prepare for, respond to, and recover from any potential threats or disruptions that may affect the postal service, such as natural disasters, accidents or cyberattacks.
[10] A security breach is an event that compromises the confidentiality, integrity, or availability of the data exchanged with other parties, such as unauthorized access, disclosure, modification, loss or destruction.

- ❑ We do not notify security breaches to any other parties
- ❑ Other (please specify):

14 How quickly do you notify the respective parties of the security breach? (Please select only one answer among the following):

- ❑ Within 24 hours
- ❑ Within 72 hours
- ❑ Within one week
- ❑ Within one month
- ❑ We do not notify any security breaches
- ❑ Other (please specify):

15 How often do you conduct security audits or assessments[11] of the infrastructure and operating environment used for the exchange of data with other parties? (Please select only one answer among the following):

- ❑ Monthly
- ❑ Quarterly
- ❑ Semi-annually
- ❑ Annually
- ❑ Never
- ❑ Other (please specify):

Part V – Data retention

16 How do you determine the retention period[12] for the personal data that you process? (Please select only one answer among the following):

- ❑ We follow the retention period of the local jurisdiction
- ❑ We follow the retention period of the most restrictive jurisdiction involved
- ❑ We retain the personal data for as long as needed

[11] Security audits or assessments are systematic evaluations of the policies, procedures and controls that protect the confidentiality, integrity and availability of the data exchanged with other parties.
[12] The retention period is the length of time that personal data is kept for the purposes of processing, storing, or archiving it, before deleting or destroying it securely.

- ❑ We retain the personal data for a fixed period of 10 years from the date of receipt
- ❑ Other (please specify):

17 How do you dispose of the personal data[13] when the retention period expires or when the personal data is no longer needed for the purposes defined? Please select all applicable options (more than one answer is possible):

- ❑ We delete the personal data from all systems and devices
- ❑ We destroy the personal data by shredding, burning, or degaussing
- ❑ We return the personal data to the sending party or transfer it to a third party authorized by the sending party
- ❑ We anonymize or aggregate the personal data to remove any personal or sensitive information
- ❑ We retain the personal data for archival, research, or statistical purposes, subject to appropriate safeguards
- ❑ Other (please specify):

Part VI – Access rights

18 What kind of data subject access rights[14] do you provide? Please select all applicable options (more than one answer is possible):

- ❑ Right to access
- ❑ Right to rectification
- ❑ Right to erasure
- ❑ Right to data portability
- ❑ Right to object
- ❑ Right to restrict processing
- ❑ No specific rights provided
- ❑ Other (please specify):

[13] Disposal of personal data means deleting, destroying, or anonymizing the personal data in a secure and irreversible manner, so that it cannot be accessed, used or disclosed by unauthorized parties.
[14] Data subject access rights are the rights that individuals may have to access, correct, delete, or restrict the processing of their personal data held by an organization.

19 How quickly do you respond[15] to requests or inquiries from other parties or directly from data subjects? (Please select only one answer among the following):

- ❑ Within one calendar day
- ❑ Within 1–3 calendar days
- ❑ Within 4–7 calendar days
- ❑ Within 2–3 weeks
- ❑ Within one month
- ❑ No specific time frame
- ❑ Other (please specify):

20 What process[16] do you have to respond to information requests from other parties or directly from data subjects? Please select all applicable options (more than one answer is possible):

- ❑ We have a formal policy and procedure to evaluate and respond to information requests from other parties, and we document and track all requests and responses
- ❑ We have general guidelines to respond to information requests from other parties, but we do not have a formal policy or procedure, and we do not document or track all requests and responses
- ❑ We do not have any specific process to respond to information requests from other parties, and we handle them on a case-by-case basis, depending on the nature and source of the request
- ❑ We do not respond to any information requests from other parties, unless we are legally required to do so
- ❑ Other (please specify):

Part VII – Record of data processing activities

21 How do you maintain your records of data processing activities[17]? What is the general format and structure of your records of data processing activities? (Please select only one answer among the following):

- ❑ We use a dedicated software tool
- ❑ We use a spreadsheet or document
- ❑ We use a physical or electronic logbook
- ❑ We do not maintain records of processing activities
- ❑ Other (please specify):

[15] A response is any communication that acknowledges, answers, or follows up on a request or inquiry from another party, such as an e-mail or a letter.
[16] Processes to respond to information requests from other parties may include steps such as receiving, verifying, prioritizing, assigning, retrieving, compiling, reviewing, approving and sending the information.
[17] Records of processing activities are documents or records that describes the personal data you collect, use, store and share as a postal operator.

22 What information about the processing activities do you gather in your records? Please select all applicable options (more than one answer is possible):

- ❑ Name and contact details of each party carrying out data processing
- ❑ Categories and sources of data being processed
- ❑ Description of technical and organizational security measures
- ❑ Other (please specify):

23 How often do you review and update your records of processing activities? (Single-select)

- ❑ At least once a year
- ❑ Every six months
- ❑ Every three months
- ❑ More frequently than every three months
- ❑ Never or rarely
- ❑ Other (please specify):

Part VIII – Training and awareness

24 Does your organization provide data protection training[18] to staff members? (Please select only one answer among the following):

- ❑ Yes, we provide regular and comprehensive data protection training programmes to all staff members
- ❑ Yes, but the training is minimal or not regularly updated
- ❑ No, our organization currently does not provide any data protection training to staff
- ❑ Other (please specify):

Part IX – Practical experience

25 Have you ever encountered any difficulties or challenges[19] in collecting, processing, transmitting or receiving data? (Please select only one answer among the following):

- ❑ Yes, frequently
- ❑ Yes, occasionally
- ❑ No, never

[18] Training includes any formalized method of educating staff members on the applicable principles, processes and responsibilities on the topic of data protection/privacy, including live training sessions, e-learning, resources and materials, etc.

[19] Difficulties or challenges may include technical issues, data quality problems, data security or privacy breaches, regulatory or legal barriers.

- ❑ I do not know
- ❑ Other (please specify):

26 If you answered yes to the previous question, what were the main causes or sources of the difficulties or challenges? Please select all applicable options (more than one answer is possible):

- ❑ Incompatible or outdated technical standards or systems
- ❑ Lack of clarity or consistency in the data requirements or formats
- ❑ Legal or regulatory barriers or restrictions
- ❑ Human or operational errors or delays
- ❑ Other (please specify):