Results of the survey on member countries' regulatory frameworks on data collection and protection[1]

Part I – General questions

1 In your national postal operations, what data protection/privacy regulation[2] are you subject to?

(87 respondents)

	Number of responses
General Data Protection Regulation (GDPR) (European Union regulation)	35
Swiss Federal Act on Data Protection (FADP)	1
California Consumer Privacy Act (CCPA)	0
Brazilian General Personal Data Protection Law (LGPD)	1
None	8
Other	47
Total	**92**[3]

2 Are there postal sector specific regulations[4] on data protection in your country?

(86 respondents)

	Number of responses
Yes	29
No	57
Total	**86**

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?

(77 respondents)

	Number of responses
Yes	24
No	53
Total	**77**

[1] Results based on responses received from 89 member countries.

[2] Data protection/privacy regulation refers to the rules and standards governing how personal data is collected, used, stored and shared.

[3] Several respondents selected multiple options in response to this question.

[4] Sector-specific regulations are those that apply only to the postal sector and may have different or additional requirements to general data protection regulations.

Ash/Hd

4 For what purposes do you collect and exchange personal data[5] with other parties in the operation of international postal services? Please select all applicable options (more than one answer is possible):

(87 respondents)

	Number of responses
Operational purposes (collection, processing, tracking/item identification, addressing, delivery, etc.)	84
Customs and security (electronic advance data, ITMATT data, etc.)	80
Quality of service (such as customer feedback and delivery performance)	49
Financial and accounting (such as billing information, payment details)	56
Other	3

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?

(87 respondents)

	Number of responses
Yes	36
No	41
Other	10
Total	**87**

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:

(87 respondents)

	Number of responses
We have a dedicated DPO or team who monitors and updates our policies and procedures regularly	59
We rely on external consultants or auditors who review and advise us on our policies and procedures periodically	3
We do not have a formal DPO or team who monitors and updates our policies and procedures regularly	21
Other	4
Total	**87**

[5] Personal data refers to any information that can be used to identify or relate to a natural person.

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):

(86 respondents)

	Number of responses
We publish our data privacy policy and notices on our website and via other communication channels	57
We conduct regular data protection impact assessments[6] and audits and report the results thereof to our stakeholders	30
We do not have a specific way of demonstrating our accountability for data privacy	21
Other	7

Part III – Information obligations

8 How do you inform data subjects[7] of the means and purposes for which their personal data is being processed?[8] Please select all applicable options (more than one answer is possible):

(87 respondents)

	Number of responses
Privacy notice	48
Terms and conditions	52
E-mail	19
Consent forms	36
None	13
Other	8

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):

(86 respondents)

	Number of responses
Regularly review and update privacy policies and consent forms to align with the specific purposes of data collection	51
Provide clear and transparent communication with data subjects regarding the intended use of their personal data and obtain explicit consent for any additional purposes	48
We have no defined method for ensuring that personal data is processed solely for the purposes for which it was gathered	18
Other	9

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

[7] 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.

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

Part IV – Confidentiality and security of data exchanges

10 How do you prevent unauthorized sharing of confidential information?[9] Please select all applicable options (more than one answer is possible):

(87 respondents)

	Number of responses
We provide regular training and awareness programmes on data privacy and confidentiality obligations	53
We have written policies and procedures that specify the roles and responsibilities of data handlers and the consequences of non-compliance	54
We use technical and organizational measures[10] to protect confidential information from unauthorized access, use, modification or disclosure	72
We monitor and audit the data-handling activities and report any breaches or incidents to the relevant authorities and parties	54
Other	3

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[11] 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:

(82 respondents)

	Number of responses
Yes, we have both an emergency plan and a backup system	69
No, we do not have an emergency plan or a backup system	10
Other	3
Total	**82**

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

[10] 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.

[11] 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.

12 How do you monitor and report any security breaches[12] related to the personal data exchanged with other parties?

(87 respondents)

	Number of responses
We have a dedicated security team or unit that monitors and reports any security breaches	40
We have a security breach response policy or procedure that guides our monitoring and reporting activities	39
We rely on the security features or alerts of our systems or networks to detect and report any security breaches	34
We do not monitor or report any security breaches	3
Other	4

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

(86 respondents)

	Number of responses
UPU International Bureau	20
Local data protection authorities	69
Affected data subjects	43
Affected counterparties	43
We do not notify security breaches to any other parties	4
Other	5

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

(87 respondents)

	Number of responses
Within 24 hours	39
Within 72 hours	29
Within one week	2
Within one month	1
We do not notify any security breaches	4
Other	12
Total	**87**

[12] 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.

15 How often do you conduct security audits or assessments[13] of the infrastructure and operating environment used for the exchange of data with other parties? Please select only one answer among the following:

(87 respondents)

	Number of responses
Monthly	10
Quarterly	8
Semi-annually	4
Annually	31
Never	10
Other	24
Total	**87**

Part V – Data retention

16 How do you determine the retention period[14] for the personal data that you process?

(87 respondents)

	Number of responses
We follow the retention period of the local jurisdiction	51
We follow the retention period of the most restrictive jurisdiction involved	7
We retain the personal data for as long as needed	28
We retain the personal data for a fixed period of 10 years from the date of receipt	5
Other	10

17 How do you dispose of the personal data[15] 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):

(87 respondents)

	Number of responses
We delete the personal data from all systems and devices	50
We destroy the personal data by shredding, burning, or degaussing	44
We return the personal data to the sending party or transfer it to a third party authorized by the sending party	10
We anonymize or aggregate the personal data to remove any personal or sensitive information	24
We retain the personal data for archival, research or statistical purposes, subject to appropriate safeguards	35
Other	8

[13] 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.
[14] 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.
[15] 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.

Part VI – Access rights

18 What kind of data subject access rights[16] do you provide? Please select all applicable options (more than one answer is possible):

(87 respondents)

	Number of responses
Right to access	60
Right to rectification	55
Right to erasure	39
Right to data portability	29
Right to object	39
Right to restrict processing	36
No specific rights provided	19
Other	4

19 How quickly do you respond[17] to requests or inquiries from other parties or directly from data subjects? Please select only one answer among the following:

(87 respondents)

	Number of responses
Within one calendar day	5
Within 1–3 calendar days	20
Within 4–7 calendar days	11
Within 2–3 weeks	5
Within one month	24
No specific time frame	13
Other	9
Total	**87**

[16] 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.
[17] 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.

20 What process[18] 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):

(86 respondents)

	Number of responses
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	54
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	9
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	22
We do not respond to any information requests from other parties, unless we are legally required to do so	5
Other	3

Part VII – Record of data processing activities

21 How do you maintain your records of data processing activities?[19] What is the general format and structure of your records of data processing activities?:

(87 respondents)

	Number of responses
We use a dedicated software tool	43
We use a spreadsheet or document	20
We use a physical or electronic logbook	9
We do not maintain records of processing activities	15
Other	4
Total	**91**[20]

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

(86 respondents)

	Number of responses
Name and contact details of each party carrying out data processing	67
Categories and sources of data being processed	47
Description of technical and organizational security measures	38
Other	24

[18] 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.
[19] Records of processing activities are documents or records that describe the personal data you collect, use, store and share as a postal operator.
[20] Several respondents selected multiple options in response to this question.

23 How often do you review and update your records of processing activities? Please select only one answer among the following:

(84 respondents)

	Number of responses
At least once a year	34
Every six months	6
Every three months	3
More frequently than every three months	10
Never or rarely	11
Other	20
Total	**84**

Part VIII – Training and awareness

24 Does your organization provide data protection training[21] to staff members? Please select only one answer among the following:

(86 respondents)

	Number of responses
Yes, we provide regular and comprehensive data protection training programmes to all staff members	51
Yes, but the training is minimal or not regularly updated	17
No, our organization currently does not provide any data protection training to staff	17
Other	1
Total	**86**

Part IX – Practical experience

25 Have you ever encountered any difficulties or challenges[22] in collecting, processing, transmitting or receiving data? Please select only one answer among the following:

(85 respondents)

	Number of responses
Yes, frequently	10
Yes, occasionally	50
No, never	19
I do not know	6
Other	0
Total	**85**

[21] Training includes any formalized method of educating staff members on the principles, processes and responsibilities applicable to data protection and privacy, including live training sessions, e-learnings and learning resources and materials.
[22] Difficulties or challenges may include technical issues, data quality problems, data security or privacy breaches, or regulatory or legal barriers.

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):

(60 respondents)

	Number of responses
Incompatible or outdated technical standards or systems	21
Lack of clarity or consistency in the data requirements or formats	14
Legal or regulatory barriers or restrictions	21
Human or operational errors or delays	43
Other	11