UPU UNIVERSAL POSTAL UNION

Data Collection and Protection Policies and Regulations in the International Postal Service

Contents

Glossary

AEO	Authorized Economic Operator
CCPA	California Consumer Privacy Act
CIS	Commonwealth of Independent States
DOs	Designated Operators
DPIA	Data Protection Impact Assessments
DPO	Data Protection Officer
EAD	Electronic Advance Data
EU	European Union
FADP	Swiss Federal Act on Data Protection
FAQ	Frequently Asked Questions
GDPR	European Union General Data Protection Regulation
IB	International Bureau
IPC	International Post Corporation
ISO	International Organization for Standardization
IT	Information Technology
ITMATT	ITeM ATTribute
LGPD	Brazilian General Personal Data Protection Law (Lei Geral de Proteção de Dados Pessoais)
MDSA	Multilateral Data Sharing Agreement
PLACI	Pre-Loading Advance Cargo Information
PPSA	Postal Payment Services Agreement
PTC	UPU International Bureau’s Postal Technology Centre
RoPA	Records of Processing Activities
SADC	Southern African Development Community
TOMs	Technical and Organizational Measures
UPU	Universal Postal Union
WCO	World Customs Organization

Executive Summary

This report provides an overview and analysis of the data protection practices and challenges within the postal sector, based on desk research, stakeholder interviews, and a survey of the Universal Postal Union (UPU) member countries. The report aims to identify best practices and accompanying recommendations for the UPU to facilitate a common and harmonized approach to data protection among its member countries and signatories of the Multilateral Data Sharing Agreement (MDSA). These recommendations aim to ensure that all UPU member countries are bound by a minimum level of data collection and protection regulations, at least in respect of the postal sector, particularly with a view to safeguarding the safe processing and transmission of personal data between UPU member countries in the context of international postal operations.

The report furthermore reviews the existing UPU policy and regulatory framework, in particular the provisions relating to the protection of personal data in the UPU Acts (more specifically those contained in the Universal Postal Convention, the Regulations to the Convention and the Postal Payment Services Agreement (PPSA)) as well as other instruments that relate to data protection, such as the Multilateral Data Sharing Agreement (MDSA), and the UPU Guidelines on the Exchange of Electronic Advance Data (EAD). The report highlights areas within the Convention, the Regulations to the Convention, and the MDSA that require further development or clarification, such as the definitions of security incidents and data breaches, data retention and deletion periods, the roles and responsibilities, the definition of data processing, and proposes specific amendments to those instruments.

It is evident from the desk research, interviews, and the results from the survey, that the regulatory landscape of data protection and privacy laws among UPU member countries is diverse and evolving, with varying degrees of alignment with international standards and practices. The data protection practices of UPU member countries are also varied, with some countries demonstrating a high level of compliance and accountability, while others face challenges in implementing and monitoring data protection measures.

While there is diversity and an evolving regulatory landscape in data protection practices among UPU member countries, there is also a level of convergence regarding foundational privacy principles, including data minimization, purpose limitation, and lawfulness. By leveraging the already existing framework, the UPU can strive for a more harmonized and effective approach to data protection, ensuring the secure processing and transmission of personal data between UPU member countries in international postal operations.

Finally, the report recommends that the UPU play a proactive role in facilitating dialogue, training, monitoring, and collaboration among its member countries. In what specifically pertains to domestic and regulatory initiatives, a formal dialogue between the UPU and domestic and/or regional authorities could be seen as beneficial for achieving better identification, and as appropriate, harmonization of the practices in place, while at the same time ensuring due respect of (i) the public international law commitments assumed by UPU member countries under the Acts and (ii) the specific status of the UPU as an intergovernmental organization and specialized agency of the United Nations. For example, work could be conducted to draft standardized clauses and clearer processes for international data transfers.

1. Introduction

1.1. Relevance and Aims of the Study

The UPU is an international organization that facilitates the development of worldwide postal services and provides a global network with value-added services and computerized applications for the management of international postal services. Within the international exchange of postal items, be it to facilitate postal services, customs control or security, an exchange of personal data takes place, including names and addresses of senders and recipients.

The UPU Acts, including the Universal Postal Convention (“Convention”) and the Regulations to the Convention, provide for the provisions and mandatory requirements for the international exchange of postal items and secure data exchanges. More specifically, the UPU has established principles for the processing of personal data within Article 10 of the Convention and Article 9 of the Postal Payment Services Agreement (PPSA). Additionally, the UPU has created an Agreement called the Multilateral Data Sharing Agreement (MDSA) which promotes a centralized yet voluntary approach to data exchange and security. These provisions are complemented by the national legislation of member countries and, where applicable, bilateral, or multilateral agreements.

This report's objective is to identify best practices and how UPU member countries can adhere to an agreed upon minimum standard of data collection and protection regulations in the postal sector. To achieve this objective, best practices regarding data protection throughout the UPU in the management and protection of personal data that is handled within its various systems are identified and analyzed and recommendations with accompanying practical implementations are made. It furthermore includes concrete recommendations as to further enhance the UPU policy and regulatory framework relating to data protection.

This report contains 6 main sections. The first section introduces the objectives and structure of the study and addresses the main limitations in the conduct of this project. Section 2 introduces the main concepts and principles of data protection and discusses the different regional perspectives on data protection. Section 3 provides the best practices and recommendations that aim to help UPU designated operators to develop and/or improve their personal data protection policies and practices through the implementation of a data protection management programme. Section 4 reviews the UPU policy and regulatory framework concerning data protection and presents recommendations for its further enhancement to ensure the different legal instruments remain current with the latest developments and expectations regarding the protection of personal data. Section 5 summarizes the different recommendations contained in sections 2, 3 and 4 and discusses their practical implementation. Finally, section 6 contains the conclusions.

1.2. Methodology and Scope

To achieve the objectives, the research methodology consisted of three main components: desk research, interviews, and a survey.

The desk research involved a systematic review of the relevant data protection laws and regulations and postal specific laws of the 192 UPU member countries. The review focused on the key aspects of data protection, such as data protection principles and the rights of data subjects. The desk research resulted in the creation of a consolidated database and country files.

The interviews were conducted with selected UPU stakeholders to gather insights into the current data protection challenges and opportunities within the UPU. The interviews were tailored to fit the specific role and perspective of each interviewee.

The survey was designed for UPU member countries and their designated operators (DOs) to provide contextual insights into their data protection practices. The survey questions were formulated with

consideration to the Convention and its Regulations, as well as the MDSA, and commonly known data protection principles and practices:

1. General
2. Accountability
3. Information Obligations
4. Confidentiality and Security of Data Exchanges
5. Data Retention
6. Access Rights
7. Records of Processing Activities
8. Training and Awareness
9. Practical Experience

The survey aimed to capture the current data protection practices and challenges of the member countries and their level of awareness of the UPU data protection principles. The results of the survey were consolidated and complemented with best practices and recommendations, which are intended to provide guidance and support to the UPU to improve their data collection and protection practices and complying with relevant frameworks.

1.3. Limitations of the Survey

The main limitations of this study are the following:

- The survey response rate was modest, as only 87 out of 192 UPU member countries completed the survey. This affects the representativeness and validity of the survey results and country files, and the generalizability of findings and recommendations.

- The survey results were sent to the contractor on an anonymous basis but could be reviewed based on the regions. This made the analysis more challenging, as it was not as easily possible to link the survey responses to the country files or to verify the accuracy and consistency of the information provided.

Despite the thoroughness of the research, there are inherent limitations to the approach taken. The research is based solely on information that is publicly accessible. This limitation means that the findings may not fully capture the nuances and complexities of how data protection principles are implemented and enforced in practice within each country.

Furthermore, some of the data protection legislation and related documents were not available in a language that the researchers are proficient in. Where translations were available, they were used, but there may be nuances lost in translation. In the few cases where translations were not available, the researchers were unable to include that information, potentially leading to gaps in the data.

The research also cannot provide an in-depth analysis of the practical application and enforcement of data protection principles within each country. The focus is on the legislative framework and the stated practical application and enforcement of data protection principles and rights, rather than how these are operationalized.

Data protection is a rapidly evolving field, and legal frameworks can change frequently. The research captures a snapshot in time, and there may have been developments or amendments to legislation and practice since the data was collected. While the desk research provides a valuable overview of the data protection practices of UPU member countries, it is important to recognize the limitations. The research serves as a foundational reference point for understanding the legislative landscape but may not fully reflect the complexities of implementation and enforcement across different jurisdictions.

2. Main concepts and principles of data collection and processing

This section introduces the main principles of data collection and processing and analyzes the national data protection policies against these principles.

2.1. Introduction

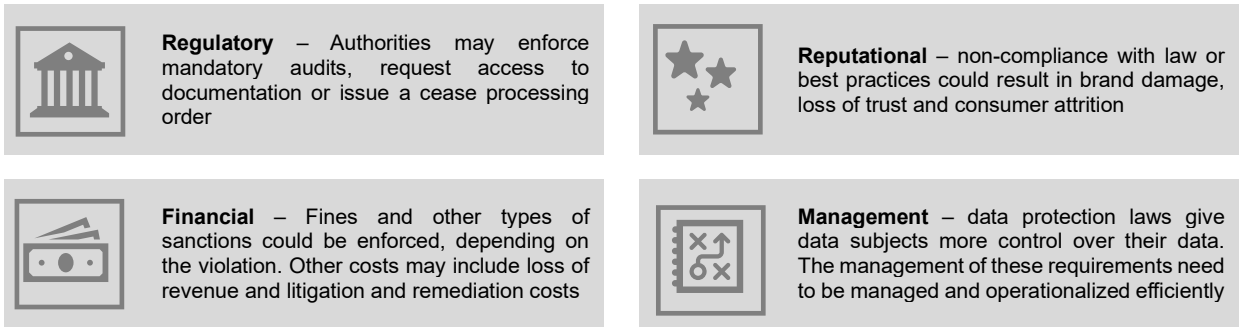
Since the 1980s, the adoption of new technologies and means of communication resulted in new opportunities for data processing on an international scale. All these developments offered considerable advantages in terms of efficiency and productivity, but also gave rise to concerns that the increased use of data, including personal data, could adversely impact on the privacy of individuals. These risks could be exacerbated when personal data more easily is transferred across international boundaries.

Like other industries, postal services have become data-driven organizations that are reliant on data to meet expectations of the market for seamless and quality end-to-end postal services. The declining cost of data collection, processing and storage, combined with the rapid accumulation of new data sources and tools have led postal operators to use data for many different purposes, including tools that enable route optimization, quality diagnostics, inquiries and strategic decision-making. Data is also collected to meet the needs of various supply chain stakeholders and to ensure operational and customer visibility of items travelling through the postal network.

Postal items are increasingly equipped with barcodes and significant amounts of information is collected on the items prior to their injection in the postal network. The total amount of electronic data comes in the form of billions of electronic data records generated by the physical movement of mail within and across borders.[1]

In a rapidly changing market and regulatory environment, data protection is critically important for the postal sector. At the national level, postal operators that do not comply with the national laws and regulations on data protection may face financial penalties or be placed under regulatory oversight. Consumers and businesses set high expectations in terms of the protection of their personal data and any breaches of the security or unlawful disclosure of their personal data to third-parties, may result in damage to brand and reputation.

Figure 1 - Various risks of an ineffective data protection management programme



2.1.1. Key definitions

[1] In this context, exclusively international mail

The fragmentation and complexity of the different data protection policies and regulatory frameworks across different regions cause significant issues in terms of compliance burdens as well as uncertainty and risk. The evolving nature of these policies and regulations may lead to inconsistent interpretations of the legal requirements by different parties such as data controllers and data subjects.

The following key definitions may be deemed as relevant from the perspective of legislative frameworks associated with the protection of the personal data .

Data subject: the individual (natural person) personal data relates to.

Personal data: any information relating to an identified or identifiable natural person ('data subject').

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Pseudonymization: processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processer: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal data breach: breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Cross-border processing: data processing that takes place in more than one country.

International data transfer: personal data transferred to a third country.

International organization: organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Privacy by Design: requires developers to integrate the protection and respect of users' privacy into the very structure of the products or services that collects personal data.

Privacy by Default: ensures the highest level of security as soon as the products or services are released, by activating by default, i.e. without any intervention from users, all the measures necessary to protect data and limit their use.

2.1.2. General data protection principles

In 1980 the Organisation for Economic Co-operation and Development (OECD) issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[2] The Guidelines have two main purposes: to reflect privacy standards and to facilitate the free flow of information for law enforcement activities. These guidelines are not legally binding but nonetheless served as a basis for future data protection policies and regulations. These guidelines aimed to strike a balance between the protection of privacy and the removal of barriers to trade allowing the uninterrupted flow of data across national borders.

[2] Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Many of the future data protection policy and regulatory frameworks contain all or most of the eight principles as outlined in the OECD guidelines, which are the following:

Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.

Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle, except: a) with the consent of the data subject; or b) by the authority of law.

Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle: Individuals (data subjects) should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
b) to have communicated to them, data relating to them
    - within a reasonable time;
    - at a charge, if any, that is not excessive;
    - in a reasonable manner; and
    - in a form that is readily intelligible to them;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed, or amended.

Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

2.2. Regional perspectives on data protection policies and principles

As more and more social and economic activities are conducted online with increasing amounts of personal data being collected, processed and transferred for the purposes of these activities, the importance of data protection is increasingly recognized around the world. According to UNCTAD (United Nations Trade and Development), as of 20 June 2024, 78% of countries have data protection legislation in force, whereas 4% have draft legislation in process and 17% of countries have no specific data protection legislation.[3]

[3] UNCTAD, Data Protection and Privacy Legislation Worldwide, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

With this global recognition, it is valuable to examine regional perspectives on data protection policies and principles. In the following sections, we will explore the data protection landscapes in different regions, including Africa, the Americas, the Arab region, the Asia-Pacific region, and Europe.

2.2.1. Africa

The African continent is the second largest and second most populous continent, after Asia in both cases. It boasts a significant cultural and legal diversity across the continent with different privacy expectations which furthermore reflect the variations in access to technology and online services, among the different African countries. Different levels of capability in areas such as technology and technology-related law and governance are other factors that can increase the difficulty of formulating and enforcing consistent policy among the various member states of this region and those of the African Union in particular. Following Mauritania's ratification on 9 May 2023, the African Union Convention on Cyber Security and Personal Data Protection (the "Malabo Convention") came into force on 8 June 2023.[4]
The Malabo Convention is unique in the world as it is the only cybersecurity treaty that combines cybersecurity, cyber-crime, electronic transactions, and data protection in one single legal instrument. For Africa, it is also the first legal instrument pertaining to digitalization to be enacted at the continental level. Since the Malabo Convention entered into force, the domestic laws of States that are party to the Convention are required to conform to the principles outlined in the instrument and to address each policy area contained therein. In fact, since its inception, the Malabo Convention has led many countries in Sub-Saharan Africa to develop or reinforce their data protection policy and regulatory frameworks, including South Africa, Nigeria, Ghana, and Kenya which have all enacted comprehensive data protection laws in accordance with the Convention's provisions.

The key principles for data protection in the Malabo Convention are:

• Consent and legitimacy,

• Lawful and fair processing,

• Purpose, relevance, and retention of data,

• Accuracy of data over its lifespan,

• Transparency of processing,

• Confidentiality and security of personal data.

Furthermore, in addition to the Malabo Convention, the Southern African Development Community (SADC) member states have also taken steps to address data protection and cybersecurity within their region. The SADC Model Law on Data Protection[5] serves as a regional guidance, providing a standardized framework for data protection in Southern Africa. The SADC Model Law closely aligns with the principles of the Malabo Convention, ensuring a consistent approach to data protection and cybersecurity across the continent. By establishing an independent authority to oversee data protection, enforcing sanctions for non-compliance, and regulating international data transfers, the SADC Model Law aims to support the implementation of the Malabo Convention at the national level within SADC countries. Additionally, it encourages the development of industry-specific codes of conduct to guide compliant data processing practices, further enhancing data protection within the region.

[4] Adopted on 27 June 2014 by the twenty-third ordinary session of the Assembly of the African Union, held in Malabo, Equatorial Guinea.
[5] SADC Model Law on Data Protection, https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf.

Kenya: DPA

The Data Protection Act (DPA), which came into force on 25 November 2019, is the primary piece of data protection legislation in Kenya. The Office of the Data Protection Commissioner (ODPC) enforces the Act. The Act is furthermore supported by the more detailed Data Protection Regulations. The DPA follows the path taken by the GDPR and often uses the same general concepts and terminology, such as “data subjects”, “controllers” and “processors”.

Malawi: DPA

The Malawi Data Protection Act (DPA) took effect in February 2024 and provide for a comprehensive legal framework for the regulation of the processing and movement of personal data of natural persons, in compliance with a range of data protection principles like fairness, transparency, data minimization, and accountability.

The existing Malawi Communications Regulatory Authority, established in 1998, was designated as the overseeing body for effective implementation and enforcement.

South Africa: POPIA

The South African Protection of Personal Information Act (POPIA) is the data protection law of South Africa. The Act passed on July 1, 2020, and came into effect one year later. Similar to the GDPR, the Act defines what personal data is and prescribes duties for controllers and processors. Although there are key differences between the GDPR and POPIA, both instruments are built on the same guiding principles of accountability, transparency, security, data minimization and the rights of data subjects.

2.2.2. Americas

The Americas, comprising North, Central, and South America, exhibit a diverse landscape when it comes to the protection of personal data. Unlike Africa or Europe, there is no harmonization of standards and principles across the various countries in the region. As a result, each country in the Americas is responsible for formulating and enforcing its own data protection policies and regulatory frameworks.

Some countries have taken proactive measures to develop or strengthen their data protection laws. For example, Brazil has enacted the General Data Protection Law (LGPD), which establishes comprehensive data protection principles and rights for individuals, as indicated below. Other countries, such as Argentina, have also made progress in enhancing their data protection frameworks.

However, although not uniformly applied or enforced across the region, there are similarities in certain principles of data protection across the Americas. These principles encompass obtaining consent and ensuring legitimacy, conducting lawful and fair processing, adhering to the purpose, relevance, and retention of data, maintaining accuracy throughout its lifespan, ensuring transparency in processing, and prioritizing the confidentiality and security of personal data.

Brazil: LGPD

The LGPG (*Lei Geral de Proteção de Dados*), was crafted to align closely with the GDPR, reflecting Brazil's commitment to data protection. Brazil's large internet market and complex regulatory landscape, with over 40 federal data privacy regulations, prompted the need for a unified approach. The LGPD aims to streamline compliance efforts and provide comprehensive protection for users and businesses. Its introduction signaled Brazil's emergence as a leader in data protection, amplifying Latin America's role in the global landscape.

Argentina: PDPA

The Personal Data Protection Act 25.326 (PDPA) or *Ley de Protección de los Datos Personales* was enacted in 2000. The PDPA sets forth the main principles and rules for the protection of personal data and has been followed by multiple decrees that detail rules for the implementation of the Act. The PDPA is aligned with international data protection standards and emphasizes principles such as consent, purpose limitation, data quality, security, and accountability.

United States

In the United States, data protection is governed by a multitude of federal and state laws, primarily focused on specific sectors like healthcare and financial services. The California Consumer Privacy Act (CCPA) is the most comprehensive data protection legislation in the US enhancing privacy rights and consumer protection of California residents. Other states (Virginia, Colorado, Connecticut, etc.). have also enacted their own privacy laws.

2.2.3. Arab region

In the Arab region, governments have been introducing significant legislation, particularly in sectors of the economy and society that heavily rely on data-driven technologies. This is evident in areas such as digital identity programs, the issuance of biometric passports, and the provision of health services.

The rapid advancement of technology and the increasing reliance on digital systems have prompted governments in the Arab region to address data protection and privacy concerns. These legislative efforts aim to establish frameworks that govern the collection, use, and storage of personal data, ensuring the protection of individuals' privacy rights. One example of such legislation is the United Arab Emirates' (UAE) Data Protection Law, which was introduced in 2020, which sets out principles and requirements for the processing of personal data. This law emphasizes consent, purpose limitation, data security, and individuals' rights, aiming to enhance data protection practices and ensure responsible handling of personal information within the UAE.

Similarly, Saudi Arabia has implemented the Personal Data Protection Law, which provides a legal framework for the protection of personal data and outlines the rights and obligations of data controllers and processors. This law aims to safeguard individuals' privacy rights and promote transparency and accountability in data processing activities.

Other countries in the Arab region, such as Bahrain, Kuwait, and Qatar, have also taken steps to address data protection concerns through the enactment of specific laws or regulations. These efforts reflect a growing recognition of the importance of data protection and privacy in the digital age.

As technology continues to advance and data-driven services become more prevalent in the Arab region, it is expected that further legislative developments will take place to ensure the protection of personal data and privacy rights. These efforts are crucial in fostering trust and confidence in digital services and promoting responsible data practices across the region.

Egypt: PDPL

Egypt published a Personal Data Protection Law (PDPL) in July 2020 that addresses the right to personal data protection and gives multiple rights to individuals. According to the Law, personal data should only be collected for specific legitimate purposes and should not be retained longer than necessary.

Organizations involved in the processing of personal information are expected to appoint an authorized Data Protection Officer (DPO).

Saudi Arabia: PDPL

In September 2021 the authorities of Saudi Arabia issued the Personal Data Protection Law (PDPL), which set stricter standards for data privacy and protection and further increased awareness around the importance of data protection compliance.

The PDPL is based on key principles such as purpose limitation and data minimization, controller obligations, including registration and maintenance of data processing records, data subject rights, and penalties for breach of provisions.

United Arab Emirates: PDPL

In November 2021, the United Arab Emirates issued Federal Law No. 45 of 2021, which set stricter standards for data privacy and protection and further increased awareness around the importance of data protection compliance. The DIFC Data Protection Law (DIFC Law No. 5 of 2020) relates to one of the UAE's free zones, Dubai International Financial Centre, and aims to safeguard the personal data of individuals whose data is processed by DIFC registered entities.

2.2.4. Asia-Pacific region

The digital economy of the Asia-Pacific region has been one of the region's success stories. At a time that trade and e-commerce generated exports are increasingly data driven, it is imperative for member countries of the Asia-Pacific region to develop robust data governance policies that are both business friendly and support cross-border data flows.
In 2016, the Association of Southeast Asian Nations, commonly abbreviated as ASEAN, adopted the Framework on Personal Data Protection establishing a set of principles to guide the implementation of measures at both national and regional levels to promote and strengthen personal data protection in the region.[6] The framework lays out the principles that the ASEAN member countries endeavor to take into account and implement in their domestic laws and regulations:

Consent, notification and purpose: An organization should not collect, use or disclose personal data about an individual unless (i) the individual has been notified of and given consent to the purpose(s) of the collection, use or disclosure of their personal data; or (ii) the collection, use or disclosure without notification or consent is authorized or required under domestic laws and regulations.

Accuracy of personal data: The personal data should be accurate and complete to the extent necessary for the purpose(s) for which the personal data is to be used or disclosed.

Security safeguards: Personal data should be appropriately protected against loss and unauthorized access, collection, use, disclosure, copying, modification, destruction or similar risks.

Access and correction: Upon request by an individual, an organization should (i) provide the individual access to their personal data which is in the possession or under the control of the organization within a reasonable period of time; and (ii) correct an error or omission in his personal data, unless domestic laws and regulations require or authorize the organization not to provide access or correct the personal data in the particular circumstances.

Transfers to Another Country or Territory: Before transferring personal data to another country or territory, the organization should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organization will protect the personal data consistently with these principles.

[6] ASEAN Framework on Personal Data Protection, https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf.

Retention: An organization should cease to retain documents containing personal data or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the retention is no longer necessary for legal or business purposes.

Accountability: An organization should be accountable for complying with measures which give effect to the principles and should, on request, provide clear and easily accessible information about its data protection policies and practices with respect to personal data in its possession or under its control. An organization should also make available information on how to contact the organization about its data protection policies and practices.

China (People's Rep.): PIPL

People's Republic of China passed the Personal Information Protection Law (PIPL) in November 2021. The PIPL regulates the processing of personal information and protects an individual's rights and interests in relation to personal information.

The PIPL stipulates that the processing of personal information must abide by the principles of legality, justice, integrity, minimum necessity, openness and transparency, and the purposes of processing shall be explicit and reasonable.

Singapore: PDPA

The Personal Data Protection Act (PDPA) provides a baseline standard of protection for personal data in Singapore and comprises various requirements governing the collection, use, disclosure and care of personal data in Singapore.

The implementation of the Act is supported by a set of subsidiary legislation as well as sector-specific laws. Under the Act, similar to the GDPR, every organization is accountable for the personal data processed on their behalf by other parties or contractors.

New Zealand: Privacy Act

The Privacy Act 2020 provides the rules in New Zealand for protecting personal information. Information Privacy Principles (IPPs) in the Act govern how agencies collect, use, disclose, store, retain and give access to personal information.

The Office of the Privacy Commissioner (OPC) enforces New Zealand's Privacy Act. Similar to the GDPR, the territorial scope of the Act applies to any organization doing business in New Zealand, regardless of their actual location.

2.2.5. Europe/ CIS: Data protection principles in Europe

GDPR

The GDPR may be deemed as one of the most influential data protection frameworks due to its comprehensive scope and influence, stringent requirements, enforcement mechanisms, and role in fostering consumer trust. Its impact extends beyond the EU, influencing laws and practices worldwide.

When it comes to data protection, the European continent has historically paid particular attention to the development of policies, guidelines and legally binding rules that regulate data protection and data processing. This framework has developed over time and includes various instruments from different bodies, for example the Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108, and its modernized version from 2018. Various non-Council of Europe states such as Argentina, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay have also acceded to the treaty.

Convention 108 constitutes the first binding international instrument in the field of data protection. The EU data protection framework gives substance and amplifies the principles of Convention 108 and takes into account accession to Convention 108, notably with regard to international transfers (see in particular Recital 105 of the EU's General Data Protection Regulation – GDPR).

The GDPR is known for its stringent requirements; bearing in mind the relative economic and political weight of the EU, it may be further noted that the potential influence of European data protection standards on global postal operations could be substantial in terms of establishing a benchmark for best practices in data protection management.

Article 5 of the GDPR sets out key principles of the EU's data protection regime. These key principles are set out right at the beginning of the GDPR and they both directly and indirectly influence the other rules and obligations found throughout the legislation. These principles are as follows:

Lawfulness, fairness, and transparency: Any processing of personal data should be lawful and fair. It should be transparent to individuals that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed.

Purpose Limitation: Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data Minimization: Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy: Controllers must ensure that personal data are accurate and, where necessary, kept up to date; taking every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage Limitation: Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed.

Integrity and Confidentiality: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorized or unlawful access to or use of personal data and the equipment used for the processing and against accidental loss, destruction or damage.

Accountability: the controller is responsible for, and must be able to demonstrate, compliance with all of the aforementioned principles.

Russia: FLPD

Federal laws 160-FZ and 152-FZ, Federal Law on Personal Data (FLPD), are the primary legislation governing personal data protection in the Russian Federation. Under these instruments, data subjects are granted several rights to control and protect their personal information, including the right of access to information, right to consent, right to rectification, right to deletion (right to be forgotten), right to restriction of processing, right to data portability, right to object, automated decision-making and profiling rights, right to complain to the DPA (Roskomnadzor).

Switzerland: FADP

Switzerland adopted the revised Federal Act on Data Protection (FADP) which took effect on 1 September 2023. The FADP applies to all Swiss or foreign organizations anywhere in the world that process the data of individuals located in Switzerland. The new law aligns Switzerland's data protection regulations more closely with the EU's GDPR. Principles of responsibility (accountability), legality (data processing to be fair and lawful) and transparency (information on data processing to be accessible and understandable) form the backbone of the legislation.

United Kingdom: DPA

The Data Protection Act 2018 is the UK's implementation of the GDPR. With UK's exit from the EU on January 31, 2020, the UK GDPR is the retained EU law version of the GDPR. With effect from 1 January 2021, there are two legal texts to consider in the UK: the UK GDPR as well as the DPA 2018. The UK data protection regime retained the very similar principles, rights and obligations as those found in EU GDPR, with some noticeable differences (for example, the age of consent for children's data, which is set at 13 years old in the UK compared to 16 years old in the EU).

2.3. National Data Protection Laws and Regulations

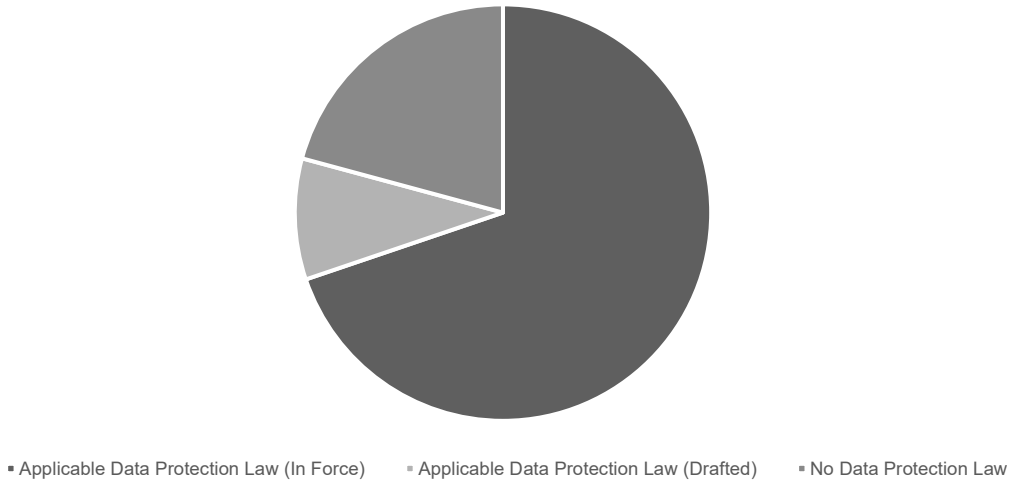
Building upon the regional overview of data protection policies and principes, it is evident that data protection laws and regulations vary significantly across different countries and regions. While each region has its own unique approach, a number of domestic and/or regional frameworks have emerged as potential benchmarks for data protection standards. The GDPR's comprehensive approach to data privacy has influenced many countries outside of the European Union (EU) to adopt similar regulations. The GDPR's emphasis on legal bases, data subject rights, and cross-border data transfer restrictions, influenced by a broad spectrum of earlier data protection concepts, including those from the OECD Guidelines, has set a high bar for privacy and data protection.

Taking a closer look at the data protection practices among the 192 member countries of the Universal Postal Union (UPU), an analysis of the data protection practices reveals a significant variance in the adoption and implementation of data protection laws and regulations. The percentage figures have been rounded to the first decimal place for evaluation.

Countries and Data Protection Laws and Regulations

A majority of the UPU member countries, representing 69.8%, or 134 member countries, have enacted data protection laws and regulations. 18 Union member countries, or 9.4%, have data protection laws and regulations drafted, but these regulations have not yet entered into force. In total, 152 member countries, have legal frameworks dedicated to data protection either in force or pending adoption and/ or implementation.

Figure 2 - Distribution of Data Protection Laws and Regulations



Approximately 20.8% of UPU member countries currently do not have applicable data protection laws and regulations. This indicates that roughly 40 countries either lack a formal legal framework for data protection or are in the very early stages of developing such laws. The absence of applicable data protection laws and regulations suggests that personal data in these countries are not subject to the same level of protection as in countries with established data protection legislation.

The disparity in data protection laws and regulations among the UPU member countries has implications for international cooperation. Countries with robust data protection laws and regulations may face challenges when exchanging data with countries that lack such protections. This could affect the efficiency and security of postal services, highlighting the need for a harmonized approach to data protection within the UPU. It should nevertheless be noted that the UPU has adopted its own legal framework, which include provisions in the UPU General Regulations, the Convention and the Postal Payment Services Agreement (PPSA) (the UPU legal framework will be discussed in section 4 of this report). It is furthermore important to note that the Acts of the Union constitute treaty-based rules for the exchanges of postal items between

member countries of the Union, including provisions that specifically prescribe the data, including personal data, that is processed by the designated operators of the Union member countries for the purposes of ensuring an efficient and quality postal service as mandated under the Acts.
The ongoing evolution of data protection laws and regulations worldwide suggests that the number of countries with enforceable laws will likely increase, reducing the gap between member countries' data protection practices. As countries with drafted legislation finalize and implement their laws, the global landscape of data protection will likely become more uniform, benefiting individuals and organizations alike.

Different multinational Data Protection and Postal Laws

A significant number of UPU member countries have a second applicable data protection legislation. This involves a national data protection law supplemented by an international framework. This includes *inter alia* the GDPR (in the case of the EU) and Convention 108, a legally binding international treaty dealing with privacy and data protection. Accession to Convention 108 is open to any country, including those outside of the Council of Europe, and it establishes the principles for data protection that signatory states must adhere to. A closer examination reveals that 48 of the member countries have additional applicable data protection laws and regulations.

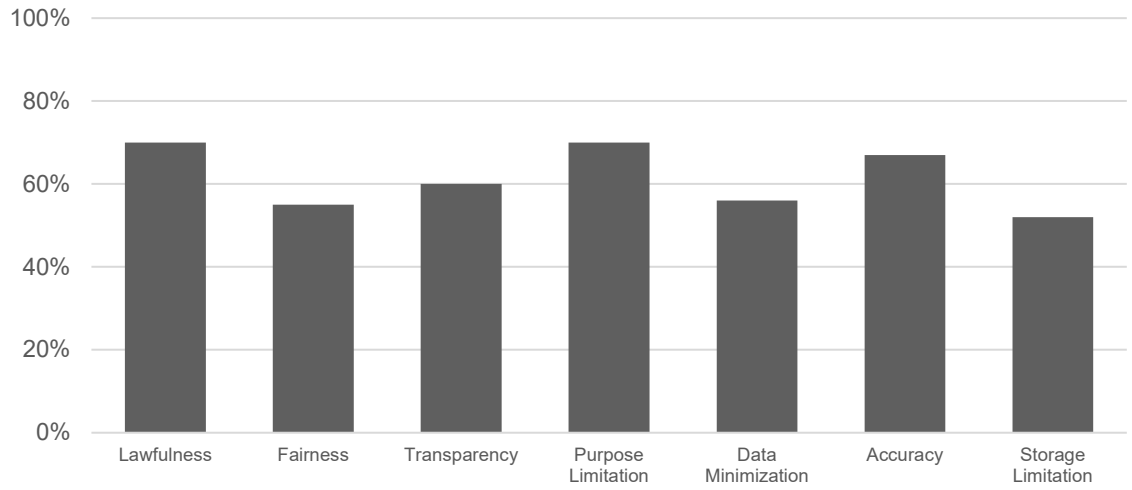
It is noteworthy that a significant number of UPU member countries – 44 in total – do not have specific postal laws in place. This absence presents a unique set of challenges and opportunities in the context of data protection. Without specific postal laws, the responsibility for data protection in the postal sector may fall under broader information privacy or data protection laws and regulations, if such exist. As such, the UPU may consider providing enhanced guidance and support for the implementation of sector-specific data protection guidelines. By addressing the legislative gaps and fostering a culture of data protection, the UPU can help ensure that the privacy and security of personal data are upheld across all member countries, thereby also maintaining the integrity and trust within the postal system.

2.4. Data Protection Principles

A number of national and international privacy frameworks have largely converged to form a set of core baseline data protection principles. The aforementioned data protection principles of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data are closely tied with national data protection legislation that have emerged in the following decades, in particular the GDPR. In this context, it may be acknowledged that the GDPR i has had a far-reaching effect, extending well beyond the borders of the EU. The core principles of the GDPR strongly overlap with those of the OECD, while, as more recent instrument, sets out more broadly the rights of individuals and imposes obligations on organizations and businesses that process personal data.

The global landscape of data protection laws and regulations has been significantly influenced by the GDPR, which serves as a benchmark for many countries. In an effort to understand the extent to which GDPR principles have been adopted, the 152 countries who have in force or drafted applicable data protection laws and regulations were analyzed. The review focused on a number of core principles introduced by the GDPR, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, and storage limitation.

Figure 3 - Distribution of Applied Data Protection Principles



- **Lawfulness**
  The principle that personal data must be processed legally and with sound legal bases for the personal data to be processed. The review indicates that most countries have incorporated this principle.

- **Fairness**
  Fairness requires that processing activities align with the reasonable expectations of data subjects. This principle is observed in roughly 55% of the countries, where the processing is expected to be done in accordance with the privacy notices provided to data subjects and in good faith.

- **Transparency**
  Transparency in data processing is essential for building trust and involves clear communication about the purpose and means of processing, the types of personal data involved, and the potential recipients of the data. The review found that 60% of the countries mandate transparency, ensuring that data subjects are adequately informed about the processing of their personal data.

- **Purpose Limitation**
  The principle of purpose limitation safeguards against the misuse of personal data by restricting its collection and processing to predefined, legitimate purposes. The review shows that close to 70% of the countries have adopted this principle.

- **Data Minimization**
  Data minimization is a principle that promotes the collection and processing of only the personal data that is necessary for the specified purposes. This principle is less widely implemented among member countries, with roughly 56% adhering to the notion that data processing should be proportionate and not excessive.

- **Accuracy**
  Ensuring the accuracy of personal data is crucial for maintaining the quality of data processing. The review shows that roughly 67% of the countries require personal data to be kept up to date and accurate.

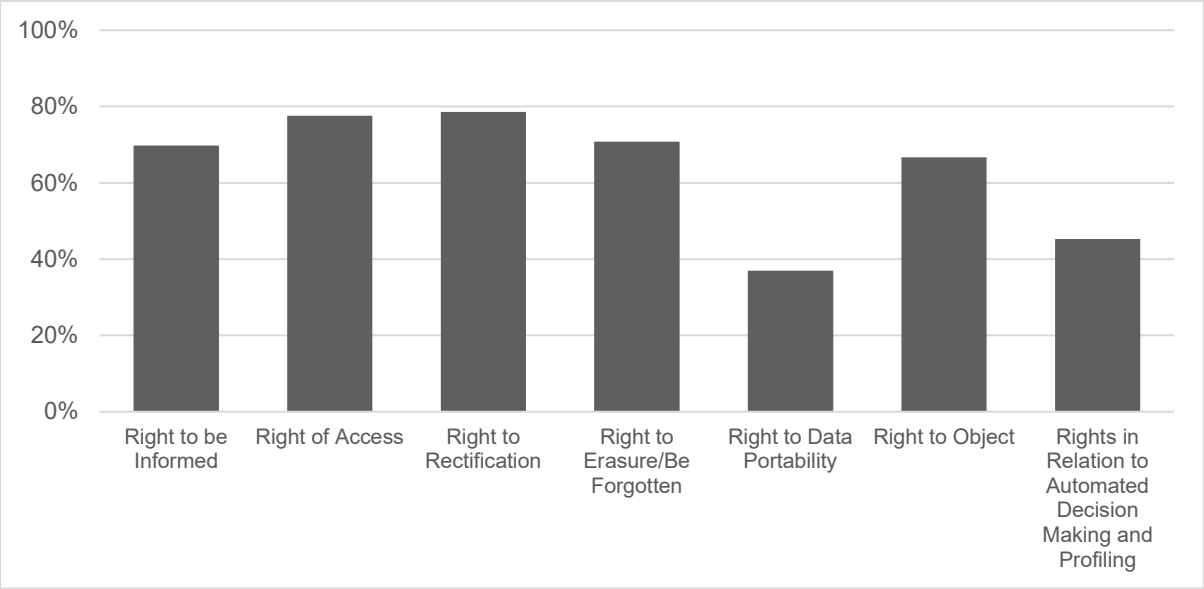
- **Storage Limitation**

The principle of storage limitation calls for the deletion of personal data once it is no longer necessary for the purpose it was collected. This principle has been adopted by 52% of the countries, reflecting a gap in how long data may be retained for and if at all deleted.

2.5. Rights Relating to Personal Data

As part of the review, the analysis also examined the perspective of data subject rights (mainly drawing from comprehensive data protection frameworks such as the GDPR. By assessing the incorporation of these rights into national frameworks of the 152 countries who have in force or drafted applicable data protection laws and regulations, a broader understanding can be gained regarding the recognition and protection of data subject rights across different jurisdictions.

Figure 4 - Distribution of Provided Data Subject Rights



Data protection regulations across various jurisdictions are designed to empower individuals with certain rights concerning their personal data. These rights are fundamental to ensuring that individuals maintain control over their personal information in an increasingly digital world. The rights typically granted to data subjects include, but are not limited to, the right to be informed, right of access, right to rectification, right to erasure and the right to object.

- **Right to be Informed**
  The right to be informed is a cornerstone of data protection in line with the principle of transparency, where there is an obligation to inform the data subjects of the nature and purpose of personal data collection. This includes disclosing the identity of those who will process the data and the intended use. Almost 70% of the member countries implement this data subject right.

- **Right of Access**
  The right of access enables data subjects to request and obtain confirmation as to whether their personal data is being processed. Upon such a request, the party with the data must provide a copy of the personal data. From the member countries reviewed, more than 77% enabled such a right.

- **Right to Rectification**
  The right to rectification addresses the need for accurate data and granting data subjects the ability to have incorrect or incomplete data corrected. This right is essential for maintaining the quality of personal data and is implemented by 78.6% of member countries, indicating a strong consensus on the importance of data accuracy.

- **Right to Erasure/Be Forgotten**
  The right to erasure, also known as the right, to be forgotten, allows data subjects to request the deletion or removal of personal data when there is no compelling reason for its continued processing. With a 70% implementation rate, this right is recognized by a significant majority of member countries, highlighting the value placed on the ability of individuals to control their digital footprint.

- **Right to Data Portability**
  A less recurring data subject right is the right to data portability, which enables data subjects to receive their personal data in a structured, commonly used format, and to transfer that data to another provider. This right is essential for fostering competition and consumer choice in the digital marketplace. Given the context of the postal service, it is understandable that this right has a lower implementation rate.

- **Right to Object**
  The right to object allows data subjects to challenge the processing of their personal data under certain circumstances, particularly when it is done without consent. A rough 66% implementation rate suggests that while this right is acknowledged by most member countries, this is not yet a commonly afforded data subject right.

- **Rights in Relation to Automated Decision Making and Profiling**
  These rights are particularly relevant in the context of data processing, where decisions can be made without human intervention. Data subjects have the right to be informed about, and to object to, automated decision-making processes that could significantly affect them. The implementation rate of 45% indicates that less than half of the member countries have fully embraced these rights, which may be attributed to divergent perspectives towards and implantation of automated processes.

Analysis reveals that while there is a general trend towards the adoption of such (or similar) data protection principles, the degree of implementation for each right varies. Notably, rights such as data portability and those related to automated decision making and profiling have lower implementation rates. It is crucial to address disparities between member countries and ensure a cohesive and comprehensive approach to data subjects' rights.

3. Building an Effective Data Protection Management Programme

The objective of this section is to help UPU designated operators develop or improve their personal data protection policies and practices through the implementation of a data protection management programme. A data protection management programme is a structured approach combining various policies and activities into a framework and life cycle to protect personal data. The stages of a data lifecycle include creation, storage, usage, sharing, archiving, and destruction. The policies and tools for implementation should aim to best protect sensitive personal data at each point of its lifecycle.

Data protection programmes are established to respond to the data protection legislation as outlined in sections 2 (national legislation) and 4 (UPU data protection framework). However, businesses are motivated, today more than ever, to ensure that they are compliant with the laws and regulations on data protection, in particular as they have interest in protection brand name, reputation and consumer trust. Data breaches and the ways in which an organization responds to such events, may lead to financial penalties, reputational damage, litigation, lost revenue, and trust.

In other words, it is critically important that designated operators review and develop their data protection programmes. Besides the legal requirements that are defined in the national context and the UPU legal framework, designated operators may consider industry best practices as standards that they may adopt. For designated operators with a relatively less or even underdeveloped data protection programme, certain quick win recommendations as outlined in this section of the report may be helpful in enhancing their capabilities.

The various aspects of a data protection programme may entail:

- Identification of data protection requirements (legal, industry practices, expectations of consumers and stakeholders),
- Review of existing policies, procedures and guidelines,
- Risk identification and mitigation,
- Establishing procedures, documentation and policies around the management of personal information,
- Raising awareness and compliance within the organization as part of a data protection-oriented culture.

An effective data protection management programme demonstrates an auditable and reliable framework to enable compliance with the various data protection policies and regulations as well as industry best-practices. Individuals and businesses would feel confident to entrust the designated operator with personal data of data subjects. Moreover, it would prevent or respond effectively to possible data breaches, thereby minimizing the risks to those individuals, businesses and the organization itself.

In 2018, the African Academic Network on Internet Policy and the Commission of the African Union, issued a report outlining the importance of ensuring trust in online services in order to sustain a productive and beneficial digital economy.[7] Designated operators collect, use and disclose personal data and are therefore required to develop and implement policies and practices that are necessary to comply with the data protection legislation in the country in which they operate.

To assist organizations in the development or improvement of their personal data protection policies and practices, the Singaporean Personal Data Protection Commission (PDPC) published a guide developing and implementing a data protection management program (PDMP).[8] The four-step data protection

[7] Personal Data Protection Guidelines for Africa, Internet Society and the Commission of the African Union, 9 May 2018, https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf.
[8] Guide to developing a data protection management programme, Personal Data Protection Commission Singapore, https://www.pdpc.gov.sg/help-and-resources/2019/07/guide-to-developing-a-data-protection-management-programme.

management programme include establishing governance and assessing risks, developing policy and practices, putting the processes into place and finally ensuring regular audits, reviews and revisions.

The PDMP and other personal data management frameworks are based on a structured life cycle approach to data protection that provides relevant methods to *measure* (assess and identify any gaps vis-à-vis data protection laws and regulations and/or industry best practices), *improve* (develop policy and practices to protect personal data), *evaluate* (sustain the policies through monitoring, auditing and communication) and *support* (respond to incidents such as data breaches) the protection of personal data.

This section of the report concerns an assessment of the UPU designated operators in terms of how their data protection management frameworks, including their policies and practices, respond to the various data protection principles as outlined in section 2. It furthermore provides recommendations for designated operators and the UPU and its member countries to further improve on the data protection management programmes, for example through capacity-building activities or the identification of best practices for the industry.

3.1. General

To gain further understanding of these data protection practices across the UPU member countries, a survey was distributed among its designated operators.[9]

The survey was designed to capture an overview of the current data protection practices across the UPU's member countries. The subsequent analysis and adaptation[10] of the results was performed to enable the identifying of collective trends and patterns of best practices and faced challenges by the postal services. Overall, 87 responses were gathered from the 192 UPU member countries. In some instances, some member countries did not provide answers to all the questions. To guarantee comparability and scalability, the feedback provided in the '*other'* option was analyzed.

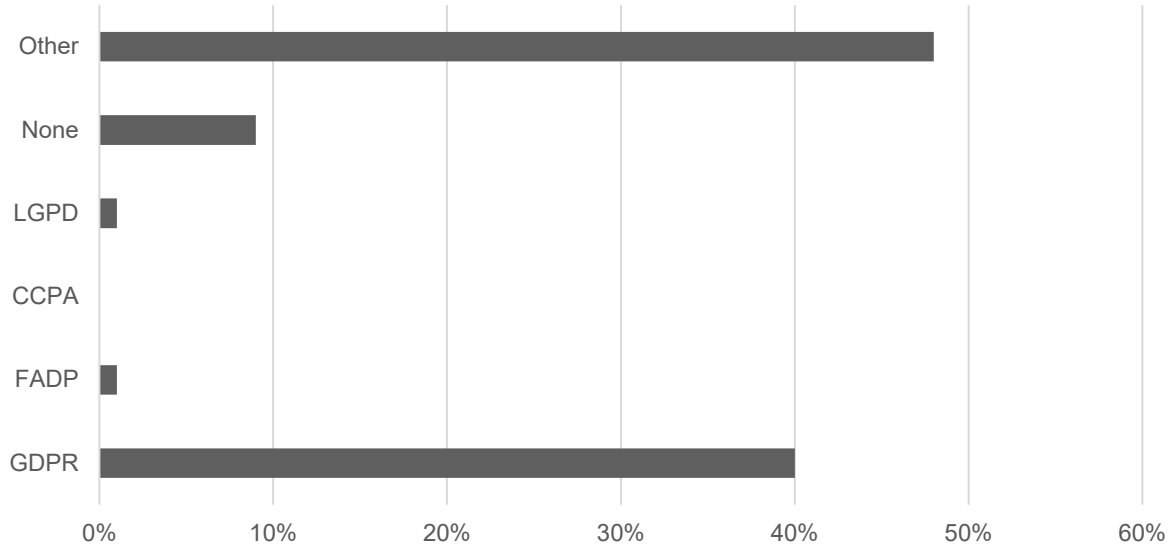
Although not all member countries responded to the survey, it is important to bear in mind that the insight from the analysis is intended to inform possible best practices and share knowledge and experiences, where possible. Furthermore, the analysis offers a snapshot in time, while setting the stage for ongoing dialogue and development in the area of data protection within the postal sector.

One of the survey objectives was to gather insights into the existing regulatory frameworks that govern the respective member countries. Specifically, it aimed to map out the laws and regulations that oversee the collection, use, and protection of personal data, thus, validating the preliminary findings that had been compiled in the country files as part of the desk research.

The survey results confirm the diverse landscape of regulatory environments. Figure 5 highlights that 40% of the respondents indicated they are subject to the GDPR (thus also meaning that 40% of the respondents are from the EU).

[9] IB circular letter 3911(DPRM.PPRE.PRA)1159 of 5 December 2023 concerning a survey on member countries' regulatory frameworks on data collection and protection.
[10] The original (raw) survey results were amended and adapted to facilitate and promote analysis and comparability, hence in certain cases, they may slightly deviate from Annex 1 of this report.

Figure 5 – Distribution of Data Protection Regulations Across Member Countries as per Survey Question 1



As already noted in section 2.2.5, and from the additional, non-GDPR responses received, a strong influence of regional frameworks such as the GDPR could be noticed.

Moreover, some countries directly subject to the GDPR also indicated adherence to their additional national legislation which confirms the layered approach to data protection discussed in section 4. This also solidifies the context in which the UPU member countries are operating and alludes to the intricacies the countries must navigate within the regulatory landscape.

Recommendation A1: To effectively navigate the complexities within the regulatory landscapes, the UPU should play a role in facilitating discussions to establish best practices and lessons learned in the area of data protection. This could be done by various means, such as organizing workshops, best practice seminars, or dedicated sessions within the existing platforms like the Postal Regulatory Forum, specifically focused on data protection. This collaborative approach will enable the identification of common trends, emerging issues, and effective solutions that can be implemented across the postal sector. Alternatively, the UPU could consider establishing a dedicated task force with a clear mandate to develop uniform data protection practices and strategies. This task force would bring together experts from member countries to collaborate on the creation of comprehensive guidelines and frameworks that promote consistent and effective data protection measures.

The survey revealed a wide variety of data protection/ privacy laws. The responses show that within the postal sector there may need to be adherence to a wide range of regulations that do not necessarily reflect one another in their entirety. With so many regulations to follow, the risk of inadvertently failing to comply with one or more of them increases. The complexity of navigating these requires ongoing training to stay updated on the latest regulations.

Recommendation A2: The UPU should adopt a harmonized and common approach to data protection based on fundamental principles of data protection.

This recommendation will ensure the smooth operation of international postal services. Such a unified approach would bolster consumer confidence but also streamline regulatory compliance for postal services operating across different jurisdictions.

A mere 9% of the countries have reported an absence of data protection regulations, suggesting that many of the postal services are governed by some form of data privacy framework. This is confirmed by the

country file. This is a positive sign for international data protection standards and suggests a global movement towards the adoption of such regulations. Conversely, this may also signify an area of potential risk. The lack of formal privacy laws could lead to weaker data protection practices, making these countries' postal services more vulnerable to data breaches and violations of data protection. To put recommendations A1 and A2 into motion, it is recommended to ensure continuous guidance and training.

Recommendation A3: The establishment and fostering of shared knowledge, guidance, training, and supplementary material is essential to cultivate a common understanding of data protection. Please also refer to recommendations A10, A14 and A28.

In addition to national legislations, a third of the respondents are also subject to postal specific regulations that acknowledge data protection requirements. This suggests that in these countries, there is a recognition of the unique nature of data handling within the postal sector, which may involve the processing of personal data.

In contrast, the absence of specific data protection regulations in the postal sector for two-thirds of the responding countries indicates that these countries might be relying on broader data protection laws and regulations that cover multiple sectors, including postal services. It could also imply that data protection in the postal sector is not yet a legislative priority in these countries, or that existing regulations are considered sufficient to cover the postal sector's data protection needs. This can lead to more disruption than harmonization among the member countries. More specifically, due to the lack of cross-sector data protection regulations in most countries, which could hinder international cooperation and trust. In return countries with stringent data protection laws and regulations may be cautious in exchanging data with countries where such protections are not as robust.

Despite the regulatory requirements, the purposes for which member countries collect personal data align with the expectations of the international postal services. To outline the purposes for data collection and processing, nearly all respondents (97%) collect and exchange personal data for operational purposes. This includes, for example, the need to track an item and deliver it to the correct address.

A slightly lower, yet still substantial, percentage of countries (92%) use personal data for customs and security purposes. This includes the exchange of EAD and ITeM ATTribute (ITMATT) data, which are critical for international security and compliance with customs regulations.

Over half of the countries (56%) collect data to monitor and improve the quality of service, such as through customer feedback and delivery performance metrics. This indicates a commitment to service improvement and customer satisfaction. Nearly two-thirds of the countries (64%) handle personal data for financial and accounting purposes, including billing information and payment details.

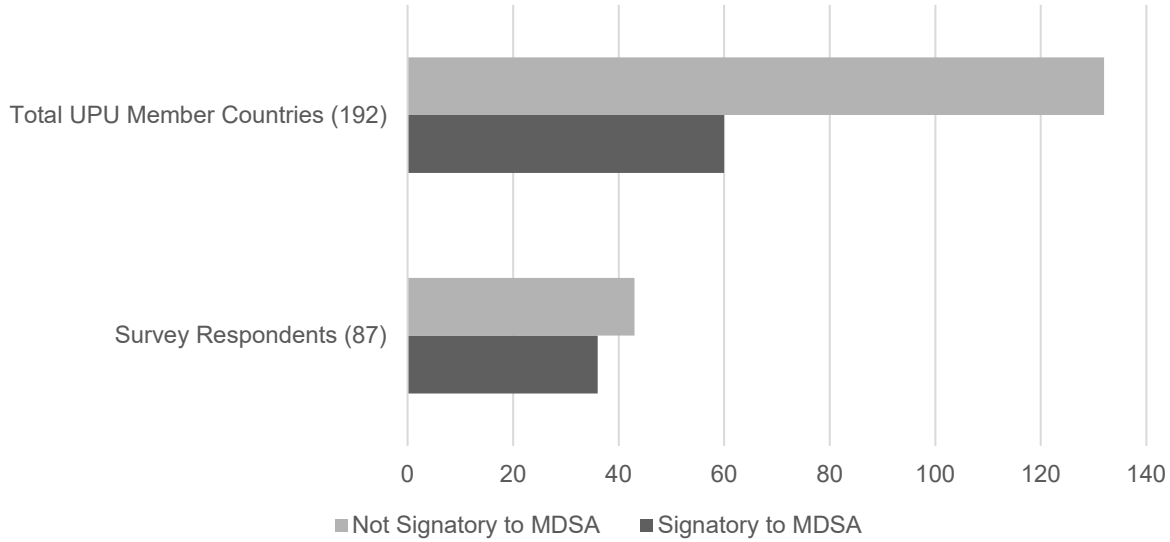
Notably, not all answer options on the purposes for processing personal data received 100% unanimous agreement among the member countries. The member countries that did not select the options often came from member countries in developing regions. It is likely that these countries tend to grapple with a range of obstacles that can impede their personal data collecting practices. Furthermore, the results show that not all respondents use data for quality of service such as customer feedback, which could lead to missed opportunities for improvement.

The pervasive use of personal data for various purposes emphasizes the need for stringent data protection and cybersecurity measures. Given the substantial volume of potentially sensitive information processed, particularly also in the context of financial transactions that may involve bank or credit card details, there is an inherent risk of exposure to fraud and theft. This risk is compounded by the global focus on security and the prevention of illegal activities, which, while necessary, also heightens the potential for personal data breaches.

As UPU member countries, it is possible to be a signatory of the MDSA. From the desk research it is known that from the 192 member countries, 60 are signatory of the MDSA. Of the 87 respondents to the survey, 36 respondents are signatories, making up 41.4% of the overall respondents. 49.4% of the

respondents are not signatories to the MDSA. This distribution, although no strong overrepresentation, must be kept in mind throughout the analysis.

Figure 6 – Distribution of Signatories to the MDSA as per the Survey Responses to Question 5 and as per the Official Signatories List



49.4% of respondents who are not signatories to the MDSA may face challenges in terms of service interoperability and data protection standards. Non-signatory countries might not be benefiting from the standardized practices and cooperative frameworks that the MDSA provides, potentially leading to inefficiencies and increased risks in handling international mail.

The 'Other' category, accounting for 9.2% of responses, includes answers to alternative existing agreements. These responses suggest that while not all members are part of the MDSA, as seen in UPU Policy and Regulatory Framework , some may still be engaged in other forms of data protection and sharing agreements, such as the International Post Corporation (IPC) Data Sharing Agreement.

Of the 60 signatories, no European or South American countries have signed the MDSA. The former could be attributed to having robust regulations and the latter could be due to contextual reasons for not joining the MDSA, such as preferring regional agreements that are more tailored to their specific needs. Nevertheless, harmonization can ensure a standardized set of mechanisms is in place to support smooth and safe processing of personal data.

Promoting the MDSA among European countries would likely have a higher chance of success if it effectively addresses their regional regulatory concerns. It is worth considering that the current MDSA may not fully address the concerns raised by the GDPR. The Schrems II ruling presents a significant challenge, as it requires GDPR compliance to ensure a level of data protection equivalent to EU standards, including limitations on government access and appropriate remedies for data subjects. Achieving these standards at a contractual level, as proposed by the MDSA, could pose considerable difficulties. Consequently, European countries may approach signing the MDSA cautiously, as they seek to ensure that it provides the necessary safeguards and mechanisms in line with the GDPR. They may also prefer to rely on regional agreements that are specifically tailored to their needs and already incorporate the high standards set by the GDPR. Nonetheless, harmonization remains crucial in establishing a standardized set of mechanisms that could support the smooth and secure processing of personal data. Yet it may be further noted that the MDSA itself already provides for the possibility of adoption of regional-specific annexes aimed at addressing more stringent parameters as applicable to certain geographical regions or groups of UPU member countries.

Recommendation A4: As indicated in UPU Policy and Regulatory Framework , it is recommended that the UPU takes proactive measures to encourage more of its member countries to become signatories to the MDSA, promoting harmonized adherence to best practices in data protection. To achieve this, it is suggested to discuss and collaborate with member countries to better understand their concrete reasons for not signing and address any potential hesitations they may have.

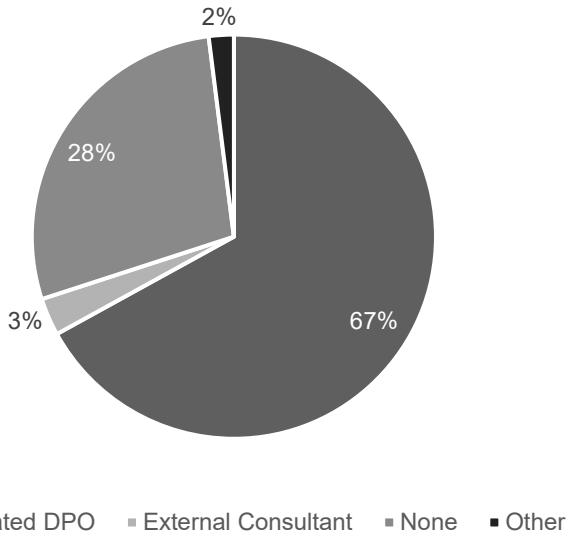
The survey responses highlight a need for the UPU to take a proactive role in ensuring that its member countries are aligned where possible in their data protection practices. By working towards harmonized data protection standards, the UPU can enhance the security and integrity of the global postal network. Taking these steps will contribute to a more robust and unified approach to data protection within the postal industry.

3.2. Accountability

Accountability in data protection refers to the responsibility delegated to handling personal data transparently and in accordance with applicable laws and regulations.

The concept of accountability is embedded in various data protection frameworks, which mandate the appointment of a DPO or a responsible person to oversee data protection strategies and ensure compliance. To explore how the member countries approach roles and responsibility, the following analysis investigates the methods employed.

Figure 7 – Distribution of Responsible Person for Ensuring Compliance per Question 6



The survey results indicate that a significant majority of the UPU member countries, specifically 67%, have a dedicated DPO or team in place. This is a strong indication that these member countries are taking data protection and privacy obligations seriously and streamlining efforts internally to ensure compliance. Having a dedicated DPO or team indicates that these countries are likely to have structured and systematic processes for ensuring compliance with data protection laws and regulations. Additionally, regular monitoring and updating of policies and procedures by these dedicated individuals or teams can lead to a robust data protection framework that can adapt to new challenges and changes in legislation.

Those with dedicated DPOs and teams tend to come from DOs that are in the Europe and Commonwealth of Independent States (CIS) Region, without distinction between developing and industrialized countries. This can be easily explained as this is a requirement of the GDPR.

Alternatively, a small percentage, 3%, rely on external consultants or auditors to review and advise on their data protection policies and procedures periodically. While this approach can provide access to specialized expertise and an external perspective, it may not offer the same level of continuous oversight and rapid response to issues that an internal DPO or team could provide. Additionally, the reliance on external parties may lead to gaps in day-to-day data protection practices due to the periodic nature of the consultations.

Here it is also worth noting that two thirds of the respondents who rely on external consultants are located amongst the developing countries in Africa and the other third come from the developing Asia-Pacific Region.

Of all responding member countries, 28% answered that they do not have a formal DPO or team that regularly monitors and updates their data protection policies and procedures. This lack of a formal role or team dedicated to data protection could potentially expose these countries to risks such as non-compliance with data protection laws and regulations, data breaches, and inadequate response mechanisms in the event of privacy-related incidents. Without a dedicated individual or team, it may be challenging for these countries to keep abreast of the evolving landscape of data protection and to implement best practices effectively. The result shows that only developing countries have answered that they do not have a person responsible for ensuring compliance and almost half of the respondents are located amongst the developing countries in America and Africa.

Recommendation A5: For those member countries without a person or team responsible for ensuring data protection compliance, it is recommended to establish such a function. This will ensure a clear point of communication and responsibility for all data protection matters. The existing language used in the MDSA does not mandate the appointment of a DPO or an equivalent role. However, adhering to best practices would strongly suggest designating an individual to oversee data protection responsibilities and compliance. It is advisable to amend the MDSA to include this requirement.

Recommendation A6: For those already with dedicated data protection teams or DPOs, the sharing of best practices and experiences amongst the member countries will support in developing harmonized strategies and lessons learned. Please also refer to recommendation A1.

Although the current phrasing of the MDSA does not require a DPO or similar role, best practice would call for such a function to not only ensure harmonization but also outline a member's commitment and steps to ensure data protection and privacy. Not only can a DPO or similar be a central contact point, but can also support in raising awareness, provide guidance, handle complaints, conduct reviews, and liaise with authorities and other key stakeholders.

Member countries can also demonstrate accountability using different methods such as publishing privacy policies and notices or transparently communicating any assessments and audits conducted.

The majority of respondents (66%) indicate that they publish data privacy policy and notices. This is a key best practice that demonstrates transparency and is often the first step in showing accountability. It allows customers and partners to transparently understand how their data is being used and what measures are in place to protect it. However, it is important to note that merely publishing such a policy does not guarantee that the policy is effective or that it is being followed.

Recommendation A7: It is recommended to clearly communicate with postal service users how their personal data is being processed and the safeguards in place for data protection. This can be done in the form of a privacy notice.

A smaller percentage of respondents (34%) conduct regular data protection impact assessments (DPIA) and audits. This practice is more proactive and provides a deeper level of accountability. Regular assessments and audits can help member countries identify potential risks and implement measures to mitigate them before they lead to data breaches or other issues. Reporting the results to stakeholders further enhances trust and demonstrates a commitment to continuous improvement.

A concerning number of respondents (24%) admit to not having a specific way of demonstrating accountability for data privacy. This lack of formalized accountability measures could expose these respondents to higher risks of data breaches, non-compliance with data protection regulations, and loss of stakeholder trust. Therefore, it is crucial for these member countries to establish clear accountability mechanisms to ensure data protection. Most countries who do not demonstrate accountability are located amongst the developing countries of the Americas and Africa.

Recommendation A8: It is recommended to assess data protection practices on a regular basis to identify areas for improvement and determine what is effective.

Furthermore, a platform to share these results could be provided by the UPU with supplementary policies on how to handle certain shortcomings. This will foster further collaboration and harmonization among member countries.

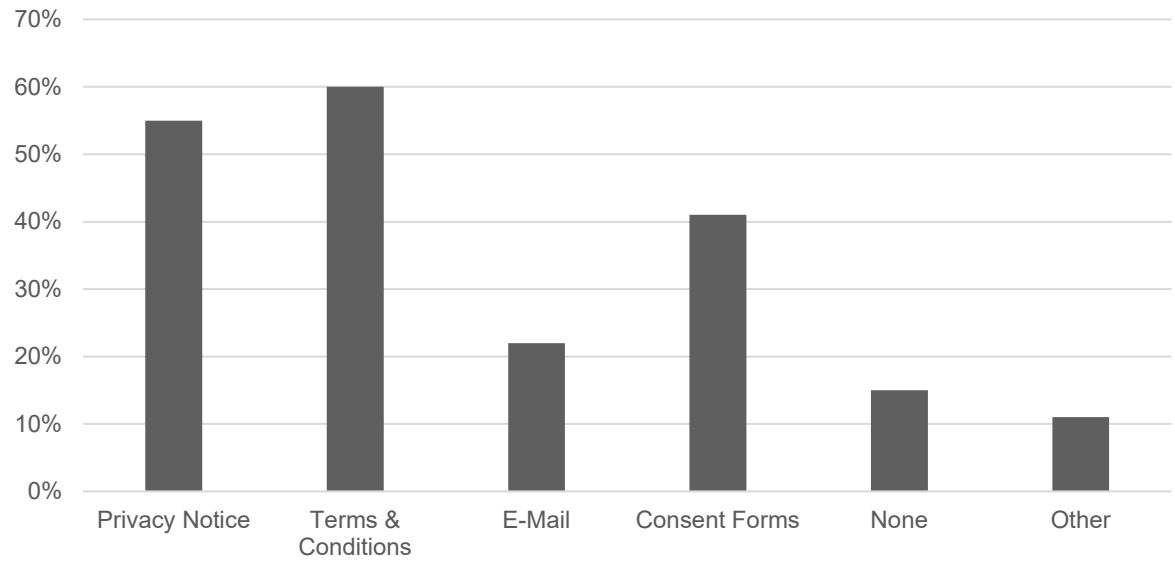
3.3. Information Obligations

In relation to the preceding topic of accountability, information obligations outline how the use of personal data will be transparently and correctly handled. Such communication can be done through privacy notices, consent forms, terms and conditions and e-mails. By implementing these information obligation mechanisms, UPU member countries can transparently demonstrate their commitment to compliantly processing personal data.

Furthermore, the information obligation is embedded in the UPU Convention Art. 10(4), which states that “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”, therefore, it is important that this is done uniformly and precisely.

The survey responses indicate a varied approach to how data subjects are informed about the processing of their personal data. The majority of respondents utilize privacy notices (55%) and terms and conditions (60%) to fulfil their information obligations. These methods are direct and typically accessible, allowing data subjects to understand the use of their personal data. However, the use of email (22%) and consent forms (41%) is less prevalent, suggesting that these methods may be supplementary or used in specific contexts where direct interaction with the data subject is possible or preferable.

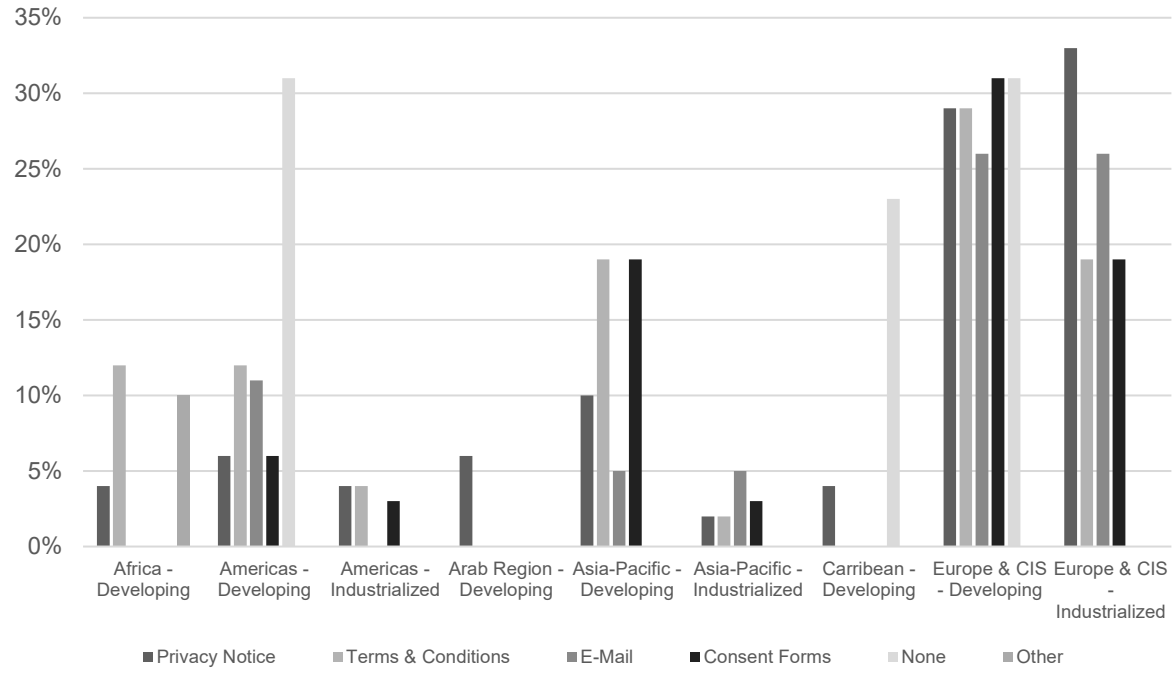
Figure 8 - Distribution of the Different Information Instruments for Data Subjects per Question 8



The fact that 15% of respondents indicated they do not inform data subjects at all is concerning, as it suggests non-compliance with the UPU Convention's Article 10(4).

Figure 9 - Distribution of Information Instruments per Region and Development Level per Question 8 showcases the distribution of where the non-compliance is more pronounced. There is a tendency for developing countries within the Europe and CIS, the Americas, and the Caribbean region to not have sufficient practices in place to meet their information obligations. The lack of uniformity in the application of information obligations could lead to inconsistencies in data protection practices and potentially undermine the trust of data subjects in the postal services provided by DOs.

Figure 9 - Distribution of Information Instruments per Region and Development Level per Question 8



Recommendation A9: To unify information obligations, the UPU could create guidelines for privacy notices and terms and conditions, that would be customizable to the specific needs of the postal sector.

The implications of these findings are significant for the UPU and its member countries. The variation in practices and the identified non-compliance with the Convention could lead to legal and reputational risks for DOs, especially in an era where data protection is increasingly scrutinized. Furthermore, the lack of a standardized approach on how to fulfil the Convention's requirement may hinder the ability for DOs to operate efficiently across borders and achieve a common level of implementation among member countries. Information obligations are a fundamental piece of the framework of data privacy rights and should be implemented in all member countries according to the Convention.

Recommendation A10: To enhance the universal understanding of data protection practices among all member countries, the UPU should offer training and resources to DOs, particularly in the developing regions, through workshops and webinars regarding the data protection requirements in the Convention. Please also refer to recommendations A3, A14 and A28.

It is critical to ensure a uniform understanding and implementation of the appropriate requirements described in the Convention and its Regulations. To ensure a uniform understanding it is recommended to regularly monitor the efforts that are implemented by each member country.

Recommendation A11: A monitoring mechanism should be in place to ensure that all member countries are adhering to their information and data protection obligations and are updating their information instruments regularly. This could involve regular surveys, audits, or peer reviews.

As previously outlined, the purposes for which data is processed among the member countries aligns with the expectations. The survey results indicate that while there is a general adherence to the principle of processing personal data only for its intended purposes among member countries, there is still room for enhancement in this practice. A level of dedication to this principle is demonstrated, yet the findings also highlight potential areas that could benefit from further improvement.

The fact that 59% of respondents regularly review and update privacy policies and consent forms is a positive indication for proactivity in aligning their data handling practices with the specific purposes of data collection.

Recommendation A12: All member countries should be encouraged to regularly review and update their privacy policies and consent forms. This should be done not only in response to changes in data processing activities but also to reflect changes in the legal and regulatory landscape.

With 55% of respondents providing clear and transparent communication to data subjects and obtaining explicit consent for additional purposes, there is evidence of a strong commitment to the principles of transparency and consent. This practice not only builds trust with data subjects but also ensures that member countries and DOs are less likely to face legal challenges related to unauthorized data use.

The 21% of respondents who indicated that they have no defined method for ensuring that personal data is processed solely for the intended purposes represent a significant risk. This lack of a systematic approach could lead to data misuse, breaches of privacy, and potential non-compliance.

Recommendation A13: To ensure compliance with Art. 10(1) of the UPU Convention, which outlines the purpose limitation for data processing, it is crucial to develop and implement systematic processes to ensure data is used only for its intended purposes.

The variety of other methods mentioned under 'Other,' such as national acts, internal controls, DPIA, and audits, reflect a multifaceted approach to data protection. These methods are indicative of efforts to comply with specific national regulations and best practices.

3.4. Confidentiality and Security of Data Exchanges

Confidentiality and the security of data exchanges are outlined in the MDSA Article 10 but is also essential for maintaining trust and safeguarding the privacy of individuals. The significance of these practices cannot be overstated. As postal services increasingly intertwine with electronic communication, the volume of data being processed and exchanged is significant. This data, often relating to postal addresses and names, is an attractive target for unauthorized access and misuse. Therefore, the UPU's commitment to robust data protection practices is critical in preserving the confidentiality and security of this data. The survey responses from UPU member countries regarding their data protection practices reveal a multi-faceted approach to preventing unauthorized sharing of confidential information.

Of the respondents, 61% provide regular training and awareness programs which suggests a strong recognition of the human factor in data protection. Regular training can significantly reduce the risk of data breaches caused by human error or negligence. Nevertheless, 39% of countries do not offer regular training and awareness programs.

Recommendation A14: Implement and foster continuous data protection training programs specially focusing on improving the confidentiality and security of data exchanges. Please also refer to recommendations A3, A10 and A28.

Clearly defined roles and responsibilities are crucial, particularly when it comes to the confidentiality and security of data exchanges as such definitions support safeguarding the personal data in a streamlined manner against unauthorized access and potential misuse. By establishing clear expectations and frameworks for accountability, the UPU ensures that member countries maintain the best practices. 62% of the respondents have written policies and procedures defining these roles, thus, there is an indication of a formal approach to data governance.

Recommendation A15: All member countries should be encouraged to develop comprehensive written policies and procedures pertaining to roles and responsibilities. These documents should be regularly reviewed and updated to reflect current best practices and legal requirements.

In addition to appropriate governance, personal data shall be protected from a technological point of view. This is done through a variety of technological measures known as TOMs. These measures encompass a broad range of security practices, from encryption and access controls to security audits and physical security measures. Most respondents, 83% use TOMs, indicating a strong reliance on these methods to safeguard personal data. This is likely testament to national legislations as the TOMs are only briefly highlighted in Article 9 of the MDSA. As touched upon, the MDSA could further clarify what TOMs are recommended to guarantee a specific level of security appropriate to the risk.

Recommendation A16: Continual investment in and updating of technical measures are crucial as threats evolve. For those not using these measures, action is recommended to implement robust technical defenses.

Furthermore, 62% of respondents monitor and audit data handling activities. This indicates a proactive stance in identifying and responding to potential data breaches. Such monitoring mechanisms are critical for early detection of security incidents. For those not currently monitoring and auditing their data protection practices, please refer to recommendation A8.

The 'Other' category was selected by 3% of respondents, with one country indicating no preventive measures in place, which is a significant concern. Although recommended to all member countries, there is one country with no preventive measures and thus should adopt a comprehensive data protection strategy.

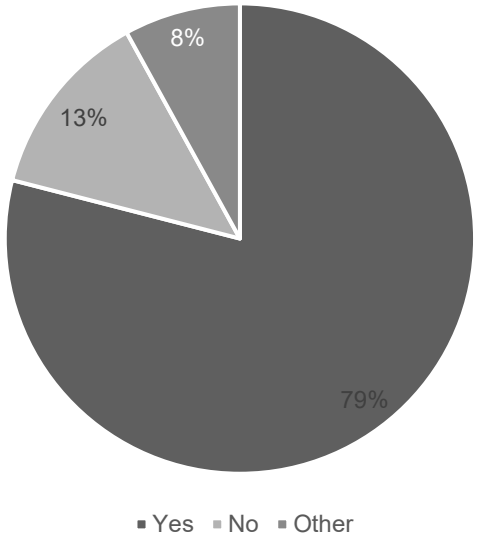
Recommendation A17: All member countries must have a data protection strategy.

Nevertheless, it can be concluded that an overall a good understanding exists surrounding the importance of protecting personal data and that many countries have measures in place to provide for the necessary security of such data.

As indicated in Article 7(3) of the MDSA, “Parties shall have an emergency plan and a backup system to enable the continuity of the service […] in case of an unplanned interruption […]”. This is in place to minimize the risk of data loss and enact responsive plans to quickly restore services. Of the MDSA signatory countries, 25 have responded that they have such an emergency plan and backup system in place leaving 11 countries do not adhere to this requirement.

However, the survey responses indicate that a majority of all the member countries (79%) have both an emergency plan and a backup system in place. This is a positive takeaway, as it suggests that these countries are prepared to handle unplanned interruptions, ensuring the continued availability of the data. Having such measures in place is crucial for maintaining the integrity of postal operations and protecting data against loss or damage due to unforeseen events.

Figure 10 – Distribution of Responses to the Existence of an Emergency Plan and Backup System per Question 11



However, 13% of the responding member countries do not have an emergency plan or a backup system. These responses come from countries across the Americas, Africa, and the Asia-Pacific regions. The lack of such plans and systems in place could lead to significant disruptions in postal services during emergencies, thereby also potentially leading to data loss, delays in delivery, and loss of trust. Nevertheless, there may be contextual reasons for the lack of such processes.

Importantly, of these countries not having an emergency plan or back up system, 73% are signatories of the MDSA. This constitutes a misalignment with the MDSA and should be remedied as soon as possible.

Recommendation A18: Immediate action is required to address and understand the gaps in emergency plans and backup systems to ensure adherence to the MDSA and preparedness against potential outages.

These findings serve as a call to action for member countries to prioritize the implementation of robust emergency and recovery protocols, thereby safeguarding the integrity and trust in the postal system.

Member countries are mandated to maintain a vigilant stance on the security of data exchanges, a responsibility that is underscored by the necessity to uphold the confidentiality and integrity of personal data shared across borders. In case of a data breach, swift action is needed as per Article 7(4) of the

MDSA. This ensures that any compromise in data security is promptly communicated but also accompanied by a resolution plan within 72 hours.

40% of respondents indicate the presence of a dedicated security team or unit to handle data security. This suggests a proactive stance, as dedicated teams are likely to be more efficient in identifying and responding to security incidents.

45% of the respondents have a security breach response policy or procedure in place. This indicates a strategic approach to data protection. Such policies typically outline the steps to be taken in the event of a breach, which can help in ensuring a timely and coordinated response.

A combined 39% of respondents rely on the security features or alerts of their systems or networks. This reliance on technology for detection is beneficial but could also be a potential weakness if not paired with human oversight, as automated systems can sometimes fail to detect sophisticated breaches.

Three of the respondents (3% of all responses) do not monitor or report any security breaches, where two respondents are signatory countries of the MDSA where it is required to notify any security incidents within 72 hours. This is a critical area of concern possibly furthered due to the lack of definitions of such incidents within the MDSA, as highlighted in UPU Policy and Regulatory Framework .

As responses from 24 signatories of the MDSA are missing, it can be assumed that more of these countries might also not have a sufficient response plan in place in accordance with the requirements set out in MDSA.

Recommendation A19: All countries responding that they do not monitor or report security incidents, especially for those subject to the MDSA, should take immediate action to establish a monitoring and reporting mechanism for security breaches relating to personal data.

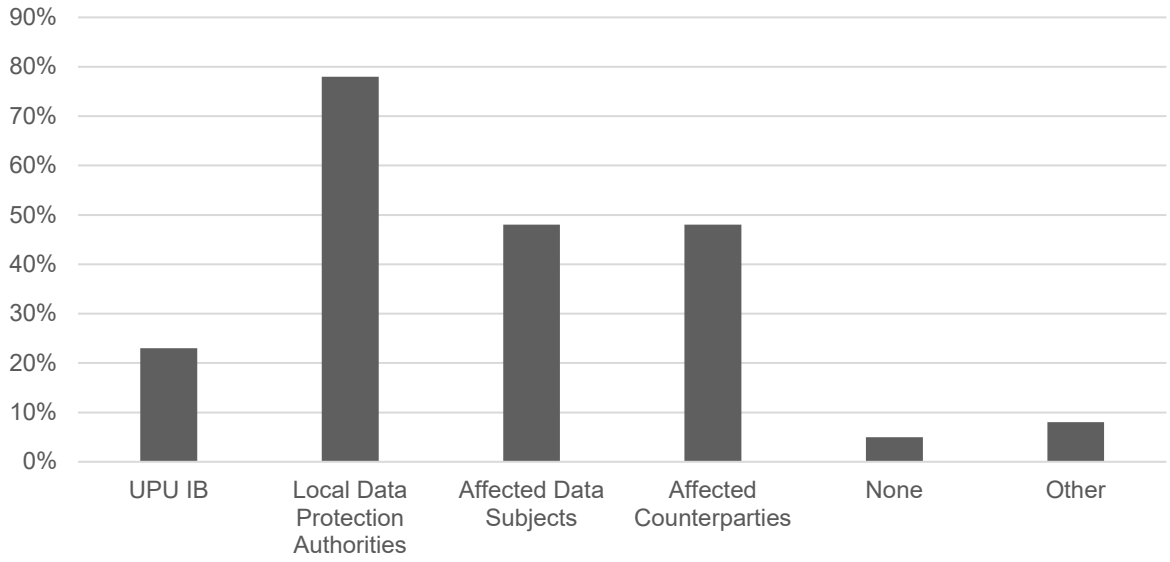
In conclusion, while the survey results show a commendable level of commitment to data protection among UPU member countries, there is room for improvement, particularly in ensuring full compliance with the MDSA and in strengthening the mechanisms for monitoring and reporting security breaches.

It is essential for all member countries to not only have robust systems in place but also to ensure that these systems are effectively integrated, and that all involved are well-trained to respond to incidents in a timely manner.

In the event of a security incident, the notification process is a critical step. The responses reveal a range of approaches on who needs to be notified, with a significant emphasis on notifying local data protection authorities, likely stemming from local regulatory requirements.

78% of respondents indicate that they notify local data protection authorities, there is a strong adherence to regulatory requirements, likely reflecting the legal obligations in many jurisdictions to report breaches. This high percentage suggests a proficient level of compliance with data protection laws and regulations, such as the GDPR in the EU, which mandates such notifications.

Figure 11 – Distribution of Notified Parties in Case of Security Breaches as per Question 13



Notifying affected data subjects is a critical step in breach response, yet only 48% of respondents do so. This is concerning as it implies that over half of the member countries may not be transparent with individuals whose personal data has been compromised, potentially exacerbating the impact of the breach and undermining trust.

Recommendation A20: All member countries should adopt a policy to outline who needs to be notified in case of security incidents and data breaches.

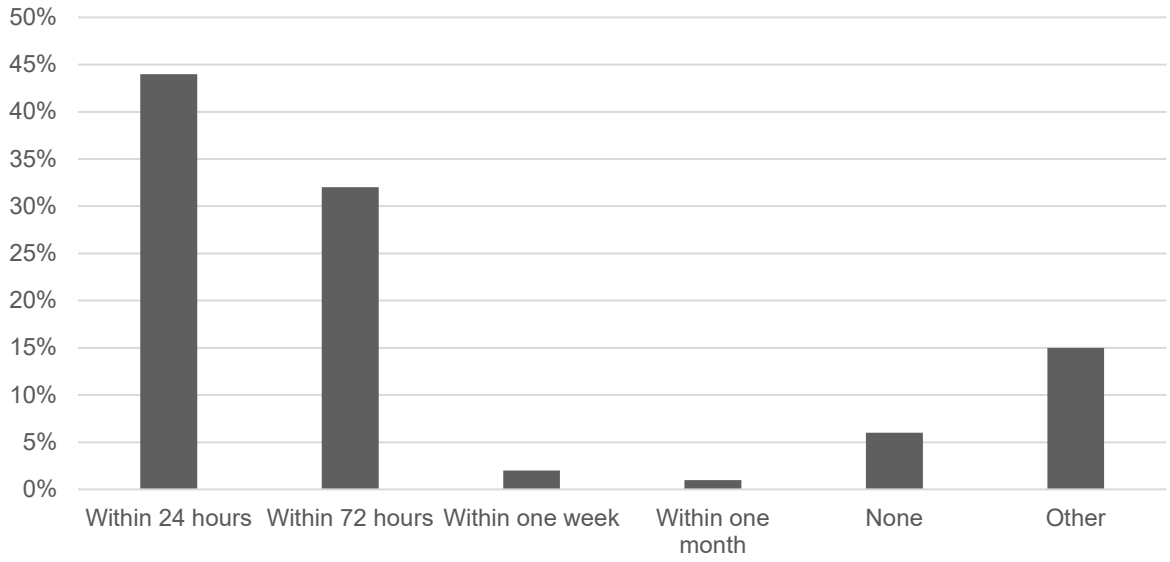
Similarly, 48% of respondents notify affected counterparties. Here it is essential to note that while Art. 7(4) of the MDSA mandates the reporting of security incidents within 72 hours to the counterparties, only 15 of the 36 responding signatory countries have answered that they do notify them. More than half of the signatories therefore have no such notification process in place which constitutes a breach with the MDSA. 5% of the respondents do not notify any parties at all. The lack of notification could lead to unmitigated risks and further spread of the incident's impact. This calls for additional guidance and policies to strengthen the responses to data breaches and security incidents.

In the 8% of responses which indicated 'Other', comments were made suggesting that some member countries follow up on notifications with internal investigations and accountability measures or that the notification to parties depends on the nature and affected persons of the breach. The former suggests a commitment to improving data protection practices and preventing future incidents.

In relation to the response times, the results indicate a strong adherence to stringent notification timelines. The reference to Art. 33 of the GDPR by some respondents underscores the influence of this Regulation, which mandates notification to the supervisory authority within 72 hours of becoming aware of a data breach. Non-compliance with such regulations can result in substantial fines and legal repercussions.

Prompt notification is often associated with transparency and can help maintain or restore trust among stakeholders. A total of 76% respondents (comprising of 44% notifying within 24 hours and 32% notifying within 72 hours) adhere to notification periods that comply with the GDPR as well as Art. 7(4) of the MDSA.

Figure 12 – Distribution of the Prescribed Period for Notification as per Question 14



Taking a closer look at the MDSA signatory countries, 29 of the 36 responses indicate a compliant response period. Nevertheless, there are 3 countries that stand out for their lack of notification, showing no adherence to any timeframes. Additionally, there is a single country that has indicated a response time of within one week. The data also presents some ambiguities and gaps. One country's response time remains unclear, providing no specific timeframe for their compliance status. Furthermore, there are 2 countries without a response.

Recommendation A21: It is recommended to enhance clarity regarding the definition of security incidents or data breaches to potentially improve response times.

Security incidents and data breaches can have significant negative impacts, including damage to reputation, legal consequences, and financial loss. These are often the result of vulnerabilities within the security landscape. To mitigate the risk of such incidents and effectively respond when they do occur, it is critical that member countries and their DOs proactively engage in security audits and assessments.

The survey results indicate a wide range of practices among UPU member countries regarding the frequency of security audits or assessments. The most common frequency is annually, with 36% of respondents following this schedule. Monthly audits are conducted by 11% of the respondents, which suggests a high level of vigilance and commitment to security within those organizations. Quarterly and semi-annual audits are less common, with 9% and 5%, respectively. Notably, 13% of respondents never conduct security audits, which poses a significant risk regarding the protection of data.

26% responded as the 'Other' category encompasses a range of practices, including risk-based approaches, irregular intervals, and audits triggered by specific events such as significant system changes or regulatory demands. Some conduct daily or weekly checks on certain aspects of their infrastructure, such as firewall checks, while others rely on external certifications and assessments, like International Organization for Standardization (ISO) audits or supplier-based vulnerability scanning.

The varied responses suggest differing levels of maturity in data protection practices among UPU member countries. The reliance on suppliers for vulnerability scanning by some respondents could indicate a lack of internal capabilities or resources dedicated to security assessments. The 13% of respondents who never conduct audits are at a higher risk of undetected security vulnerabilities, which could lead to data breaches and loss of trust from stakeholders.

Recommendation A22: As a best practice, establish a plan and timeframe for regular security assessments as part of an overarching security assessment policy.

Those who conduct regular audits, whether annually or more frequently, are likely to be more aware of their security and better prepared to respond to threats. However, the effectiveness of these audits depends on their thoroughness and the subsequent actions taken to address identified vulnerabilities.

Establishing a schedule for security audits, with a minimum of one comprehensive audit per year, is widely regarded as a best practice. These audits serve a vital role in pinpointing security weaknesses and verifying that all protective measures are current and effective.

The effectiveness of security audits can be significantly hampered by poor cooperation among stakeholders. This is highlighted by the feedback received outlining a request for a better collaboration with the UPU International Bureau's Postal Technology Center (PTC). To address this issue, it is imperative to foster communication and cooperation between all parties involved. This may involve the establishment of more explicit communication channels and clearly defined responsibilities. A proactive approach on security can significantly reduce the window of opportunity for potential breaches and ensure a robust defense against threats.

3.5. Data Retention

Data retention is a critical part of purpose limitation. Data retention strikes a delicate balance between the need to preserve data for the purposes defined and the imperative to protect individuals' rights to privacy. Article 8 of the MDSA highlights the approach in determining retention periods in accordance with national applicable laws and reasonable assumptions.

To further understand current practices, respondents were asked to provide further detail on how the retention period for personal data is determined, as well as how personal data is being disposed of when the retention period expires or when the personal data is no longer needed for the purposes defined.

Many respondents (61%) adhere to the retention period of their local jurisdiction. This approach suggests a compliance-focused strategy that aligns with national laws. However, it may not account for international obligations. A small percentage (8%) follow the retention period of the most restrictive jurisdiction involved. This conservative approach minimizes the risk of non-compliance with international data protection laws and regulations but may result in unnecessarily short retention periods, which could affect operational efficiency.

32% of respondents indicated that they retain personal data for as long as it is deemed necessary. This introduces a level of subjectivity and potential inconsistency in retention practices. This could lead to data being held longer than legally permitted or necessary, thus increasing the risk of data breaches and non-compliance with data protection regulations.

A fixed retention period (6%), such as 10 years, provides clarity and uniformity but may not align with the varying requirements of different jurisdictions or the principles of data minimization and storage limitation. The variety of 'Other' responses (9%) indicates a lack of standardization in retention practices. Responses stating "archive" and "reasonable level" do not provide an insight into clear retention frameworks. Other responses indicated reliance on UPU software for retention decisions, which suggests a trust in the software's compliance.

Recommendation A23: It is critical to establish high-level clear retention schedules that do not supersede national and international requirements but outline best practices for those who do not have the necessary guidance from national legislation.

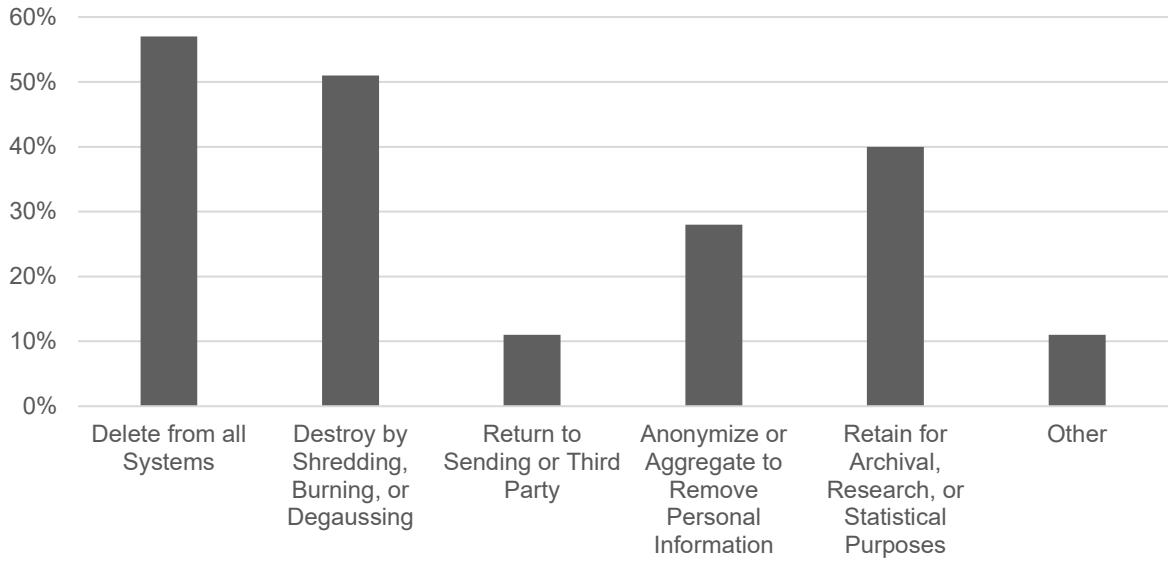
To provide for an ongoing and sustainable management of data retention, the implemented and applied retention periods should also be regularly reviewed and updated to reflect changes in legal requirements and operational needs.

Once the retention periods have expired, 57% of the respondents indicated that they delete personal data from all systems and devices. This is a best practice that aligns with many data protection regulations,

which require the secure deletion of data that is no longer necessary. However, merely deleting files may not be sufficient as deleted data can sometimes be recovered unless it is securely overwritten. Here it is important to enable and ensure clear deletion methods, such as the secure wiping of data to prevent recovery.

Once the retention period ends, clear processes are required to outline next steps concerning the adequate disposal of personal data to comply with the principle of data minimization.

Figure 13 - Distribution of Disposal of Personal Data after Expiration of Retention Period per Question 17



Over half of the respondents (51%) destroy personal data physically, where available. This method is effective in preventing data recovery. However, it is important that physical destruction be carried out securely and in an environmentally responsible manner. The development of clear guidelines for the physical destruction of data, including secure handling prior to destruction, choosing environmentally friendly methods, and maintaining records of destruction are beneficial to ensure appropriate deletion.

11% of the respondents transfer or return personal data to the sending party or an authorized third party. A higher percentage of responses (28%) indicated the anonymization or aggregation of data to retain information for analysis without compromising individual privacy. However, there is a risk of re-identification if the anonymization process is not done correctly.

Retaining personal data for archival, research, or statistical purposes (40%) can be beneficial but must be done with appropriate safeguards to protect privacy. The lack of clarity on what constitutes "appropriate safeguards" is a concern. Here it is imperative to define what safeguards are in place and to evaluate their appropriateness. These may include access controls, encryption, and regular reviews of the necessity of data retention. Furthermore, it is critical to establish clear criteria for determining when data should be archived or destroyed.

Recommendation A24: Clear guidelines and policies should be created on the proper disposal and deletion of no longer needed personal data to comply with the principles of data minimization.

By ensuring that personal data is not retained indefinitely, the risk of unauthorized access can be significantly reduced and ensure that important principles like data minimization are upheld. Furthermore, proper disposal of data no longer needed can lead to improved operational efficiency.

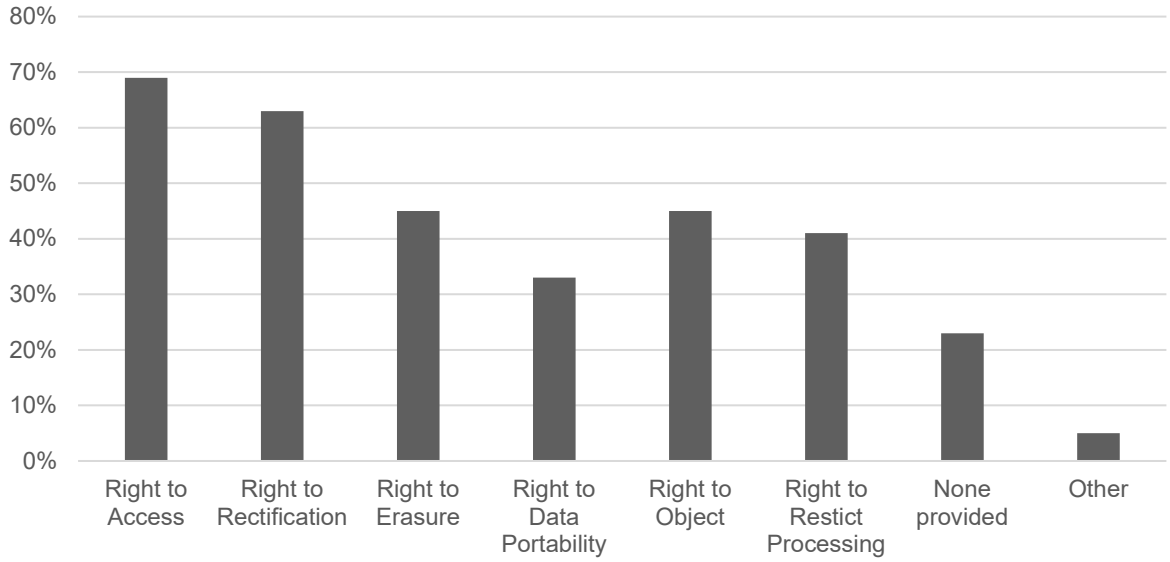
3.6. Data Subject Rights

Rights related to data are in many jurisdictions a legal requirement, nevertheless, they are a fundamental aspect of the postal operations that underpin its integrity, efficiency, and the trust it holds with clients. As the postal services become increasingly interconnected and reliant on digital communication and exchanges of data, the role the UPU and its member countries play in safeguarding personal data while facilitating international postal services becomes ever more significant.

In the context of this analysis, it is important to differentiate between the data subject rights as provided to the individual data subjects, e.g., the access right, right to rectification, and the “access right” as provided under Art. 9(1) of the MDSA. While the data subject rights are provided on the level of national legislation to individual persons, the MDSA only entails the right that one signatory country can request information from the other.

The majority of countries provide several data subject rights, with the most common being the right to access (69%) and the right to rectification (63%). These rights are fundamental to data protection practices as they empower individuals to have control over their personal data. The right to access allows individuals to see what personal data an organization holds about them, while the right to rectification enables them to correct any inaccuracies.

Figure 14 - Distribution of Provided Data Subject Rights as per Question 18



However, less than half of the countries provide the right to erasure (45%), the right to object (45%), and the right to restrict processing (41%). These rights are crucial for individuals to manage their privacy and the use of their data. The right to erasure, also known as the 'right to be forgotten', allows individuals to request the deletion of their data when it is no longer necessary or if they withdraw consent. The right to object and the right to restrict processing give individuals the power to stop or limit how their data is used, especially in cases where the data processing does not align with their interests or is done without a legitimate basis.

The right to data portability, provided by only 33% of the countries, is a newer concept introduced by the GDPR. It allows individuals to obtain and reuse their personal data across different services, facilitating control over their information and the ability to transfer it from one service provider to another.

It is concerning that 23% of the countries responded that they do not provide any specific rights to data subjects. This could be due to several reasons, such as the absence of comprehensive data protection laws and regulations, the presence of other competing legal priorities or resource constraints. In some cases, countries may not have the infrastructure or the regulatory framework in place to enforce data protection rights effectively. This can be particularly true for developing regions, where technological advancements outpace the creation of laws and regulations that would typically protect data subjects.

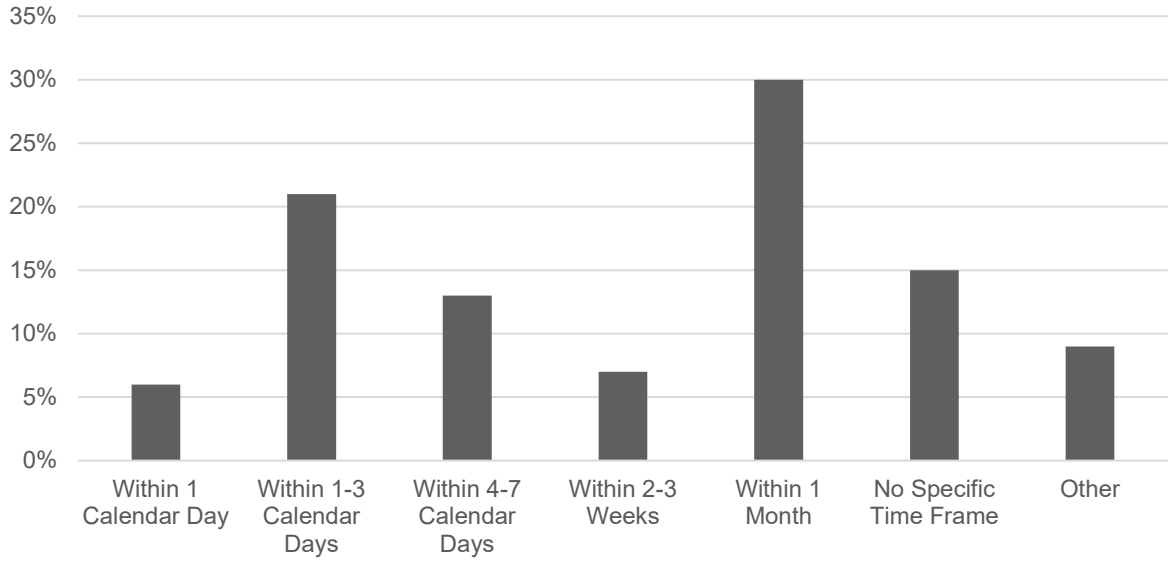
Additionally, there may be cultural factors at play that influence the perception and importance of data privacy within a country, leading to a lower emphasis on formalizing data subject rights in legislation.

Recommendation A25: In developing regions, it is important to foster a minimal level of data subject rights which can be attained.

By providing training and supplementary policies on best practices the awareness and importance of the implementation of such data subject rights can be highlighted and the process in developing them can be accelerated by the UPU.

Several jurisdictions outline the response periods for data subject requests or inquiries. 27% of the respondents respond within 1-3 calendar days. A small segment (13%) responds within 4-7 calendar days. The largest proportion of countries (37%) respond within 2-4 weeks, which aligns with best practices regarding responses to data subject right requests such as those outlined in the GDPR which stipulates a period of 30 days.

Figure 15 - Distribution of Response Periods to Requests or Inquiries from other Parties or Data Subjects as per Question 19



A significant portion (15%) of countries do not have a specific timeframe for responding to requests. This lack of defined response times could lead to unreliability and potential dissatisfaction and distrust among data subjects and other member countries.

In order to respond to such requests, many respondents indicated having a process in place. A significant majority of the responding countries (61%) have a formal policy and procedure to evaluate and respond to information requests. The countries who document and track all requests and responses are indicative of a systematic approach to data subject request management and accountability. This can enhance trust among data subjects and other parties that their information is being handled responsibly.

A small percentage of countries (6%)[11] rely on general guidelines without a formal policy or tracking system. This approach may be more flexible but could lead to inconsistencies in how requests are handled. Without documentation and tracking, it is difficult to render account that all requests are being dealt with, to audit the process or to ensure that all requests are addressed in a timely and appropriate manner.

[11] Corrected Percentage: For this question several countries have chosen the first and second answer option, however, they contradict each other. Since the first option encompasses more actions taken, the selected second option for these countries has been eliminated.

The use of a physical or electronic logbook by a quarter of the countries (25%) suggests an effort to keep records of information requests, which is a positive step towards accountability. However, the effectiveness of this method depends on the robustness of the logbook system and whether it is integrated with a wider data protection strategy.

A small percentage of countries (6%) only respond to information requests when legally mandated. This approach may comply with minimal legal standards but does not foster a proactive stance on data protection. It could potentially undermine trust with data subjects and other parties who may expect more transparency and engagement.

Recommendation A26: The UPU should promote the establishment of formal policies. This should include clear guidelines on how to respond to different types of requests, who is responsible for responding, what to document, and within what timeframe.

A regular monitoring and evaluation of the actual response times can help identify bottlenecks and areas for improvement, ensuring that data protection practices meet the needs of data subjects and adhere to international standards.

The tracking of the requests and outcomes is not only a best practice but also aids in maintaining a transparent and accountable process. It can also be useful for legal compliance and for improving data management practices over time.

3.7. Records of Processing Activities

Article 9(1) of the MDSA requires signatories to keep an updated record of all data processing activities with an identification of the data processing categories and TOMs adopted. A RoPA serves as a fundamental component of an organization's data protection strategy and framework and provides a comprehensive overview of all data processing activities. Having an up to date and regularly reviewed RoPA is seen as a regulatory requirement and best practice.

The survey results indicate a variety of approaches to maintaining RoPA among UPU member countries. A significant 48%[12] of respondents use dedicated software tools to maintain their RoPA. This suggests a trend towards digitalization and automation in data protection practices, which can enhance accuracy, efficiency, and ease of access to records. It also indicates a level of investment in data protection infrastructure. A combined 33% of respondents rely on spreadsheets, documents, or logbooks. This is a good baseline for maintaining a RoPA.

17% of countries that do not maintain a RoPA are at risk of losing oversight of their processing practices, which could lead to data quality issues and potential breaches. The lack of record-keeping could reflect a gap in data protection awareness.

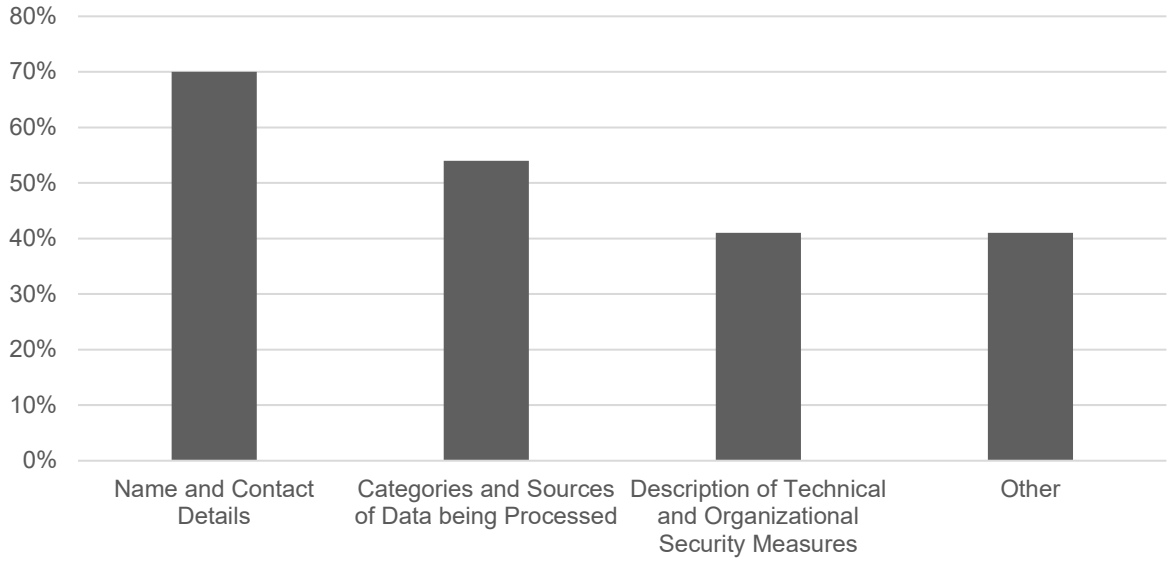
7% of the respondents chose the answer option ‘Other’. Some respondents indicated not understanding the question, as well as the term processing. This demonstrates a lack of understanding of the fundamentals of data protection and, therefore, pinpoints the imperative need to promote a universal understanding of data protection principles and definitions. The lack of clarity can lead to inconsistent practices and undermine data protection efforts.

The UPU should develop standardized training modules on data protection principles, including defining definitions such as ‘data processing’ in its Convention and Regulations. This training should be made accessible to all member countries to promote universal understanding and consistent application of data protection practices. Please refer to recommendation A3.

[12] For this question, in several cases more than one answer option was chosen by the responding countries, therefore the total percentage equals to 106%. These multiple answers are due to the fact that several tools can be used at once to maintain a RoPA.

The MDSA outlines the minimum type of information required in a RoPA. A majority of the member countries maintaining a RoPA (70%)[13] record the name and contact details of the parties that carry out data processing. This is a fundamental aspect of accountability and transparency in data processing activities, as it allows for the identification of the parties responsible for a certain processing activity and is often seen as best practice.

Figure 16 - Distribution of Gathered Information in the RoPA as per Question 22 (corrected percentages)



Over half of the respondents (54%) keep records of the categories and sources of the data that is being processed. This is crucial for understanding the scope and origin of the data, which is important for a robust risk assessment and for ensuring that all data is processed lawfully.

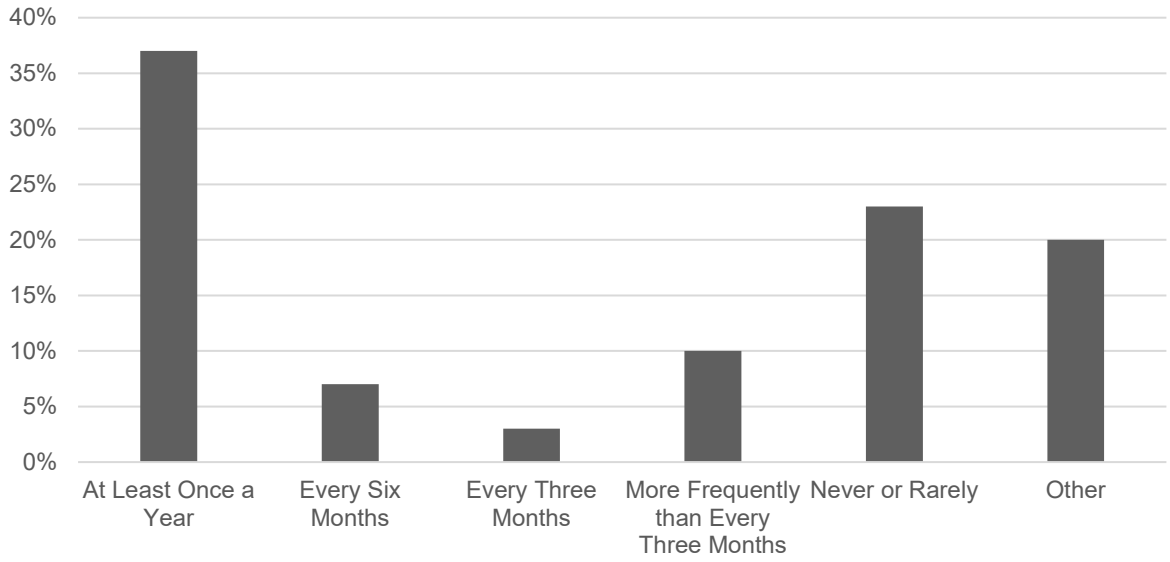
Less than half of the countries (41%) document technical and organizational security measures, albeit a requirement in the MDSA. This indicates a potential area for improvement, as documenting the implemented security measures is also essential for demonstrating compliance with data protection principles, for responding effectively to data breaches and showcasing the commitment to protecting personal data.

The 'Other' category, which includes responses such as purposes of collection, legal bases for processing, and retention periods, was noted by 41% of the respondents. This suggests that there is a significant variation in the additional information that countries consider important to document. Another explanation for the elaborated ‘Other’ responses lies in the further information required by Art. 30 of the GDPR. There, an extensive list of what information must be available for each processing activity can be found, therefore, obligating all EU member countries to provide this information.

Moreover, the survey responses from UPU member countries regarding the frequency of reviewing and updating the RoPA reveal a diverse range of practices. The frequency of reviewing the RoPA at least once a year was chosen by 37%[14] of the responding member countries. This frequency is generally considered a good practice, as it aligns with annual planning cycles and may satisfy many regulatory requirements. It suggests a proactive approach to data protection and may indicate a mature data governance framework.

[13] Corrected Percentages: Since for Question 21, several countries have answered that they do not maintain a RoPA, their responses in this follow up question have been corrected to ‘Other’ and noted down as ‘none’.
[14] Corrected Percentages: see footnote 6.

Figure 17 - Distribution of the Review and Update Frequency of the RoPA per Question 23 (corrected percentages)



The frequencies of every six months (7%) and every three months (3%) suggest a higher level of diligence and may be appropriate for those operating in a more highly regulated environment. It could also reflect a response to a higher perceived level of risk or a commitment to best practices in data protection.

Reviews more frequently than every three months were chosen by 10% of responding countries. This frequency ensures a high level of responsiveness to changes in data processing activities.

The response option 'never or rarely' was chosen by 23% of responding countries, which is a concerning response rate. This could lead to a lack of awareness of data processing activities, the potential of data breaches, how to respond to requests, and to potential complications when sharing personal data with other member countries with higher data protection requirements.

Recommendation A27: It is recommended that the UPU support its member countries by providing comprehensive guidelines on the RoPA. These guidelines should outline the obligatory pieces of information required for completion and include examples for ease of understanding. By doing so, the UPU can ensure a certain level of standardization across postal services and promote the harmonization of data protection practices in the postal sector. Additionally, it is suggested that internal guidelines be established for the frequency of reviewing and updating the RoPA, with an annual review being the commonly accepted minimum.

This would ensure a certain level of standardization across the postal services and completion of the necessary information. By doing so, the UPU could promote the facilitation of the harmonization of data protection practices in the postal sector.

Also, it is crucial to document all updates, train staff on the importance of a RoPA, comply with data protection laws and regulations like the GDPR and requirements in the MDSA, and consider leveraging technology to manage the complexity of the RoPA management. Having an updated RoPA and data mapping will improve operational efficiencies and navigate where data is and the purposes for which it is processed.

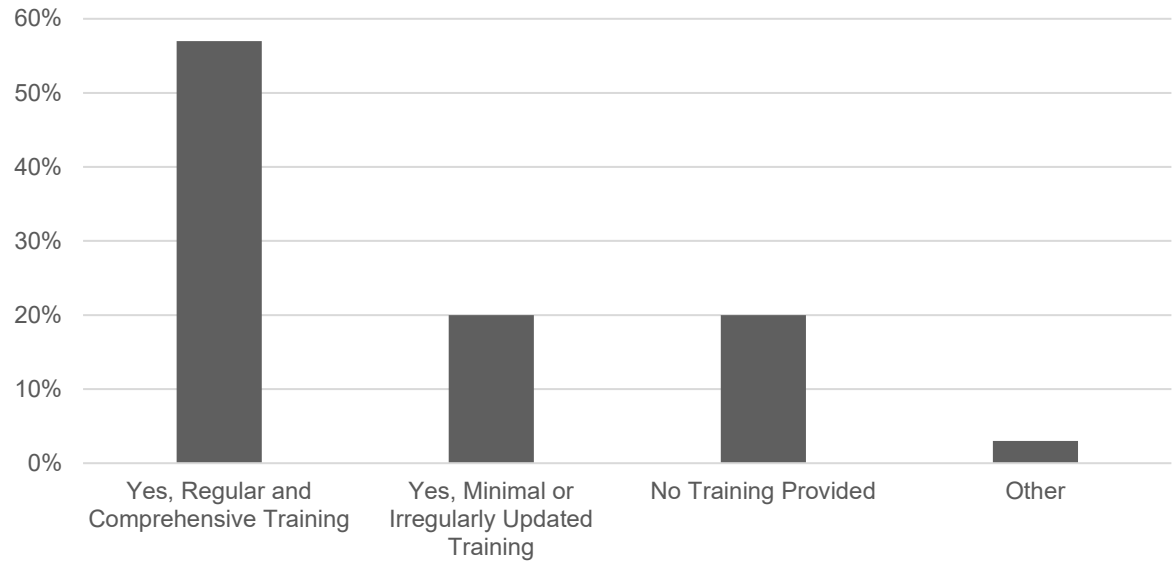
3.8. Training and Awareness

A common conclusion from the preceding sections could be bolstered through increased training and awareness. Such mechanisms serve to educate all relevant stakeholders about the importance of

protecting personal data, the potential risks associated with not doing so, such as data breaches, and the best practices for ensuring data privacy are upheld.

The survey results indicate a significant variance in the approach to data protection training among UPU member countries. With 57% of respondents affirming that they provide regular and comprehensive data protection training to all staff members, it is evident that a majority recognize the importance of such training in safeguarding data privacy and complying with data protection laws and regulations as well as best practice guidelines. However, it is important to note that overall, 77% of all responding member countries provide data protection training in some format. This is a positive indication, as it suggests that over half of the member countries are actively working to ensure that their staff is well-informed about data protection practices.

Figure 18 - Distribution of Performance and Quality of Data Protection Training per Question 24



However, the survey reveals that 20% of member countries offer minimal or irregular training, this includes two industrialized countries. Moreover, 20% do not provide any data protection training at all. This is concerning because it implies that still a significant portion of staff may be ill-equipped to handle personal data appropriately, which could lead to data breaches and non-compliance with data protection laws and regulations.

The "other" category, which encompasses 3% of the responses, indicates a more ad hoc approach to training, with new staff members receiving education on data protection measures and responsibilities, or training being provided only to certain roles or levels. Nevertheless, this suggests that data protection training is not uniformly applied across all staff, potentially creating gaps in the overall data protection strategy.

Recommendation A28: The availability of regular training can be promoted by the UPU to accelerate and ease access to data protection best practices. Please also refer to recommendations A3, A10 and A14.

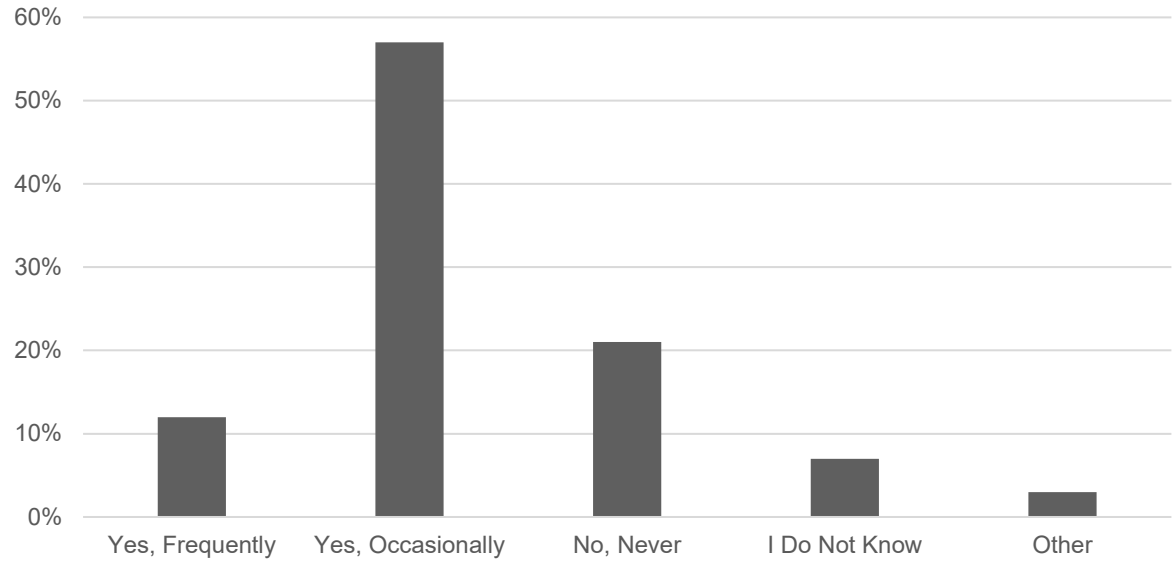
Providing training is always beneficial and is typically easy to put in place, by using webinars or recordings. This could support the member countries where data protection requirements are minimally or not at all regulated through their national legislations, to better understand the concerns and challenges faced by other member countries who must comply with more strict requirements.

3.9. Practical Experience

As part of the survey, member countries were asked to indicate if they had encountered difficulties or challenges in collecting, processing, transmitting, or receiving data and, if so, what the main causes or sources were.

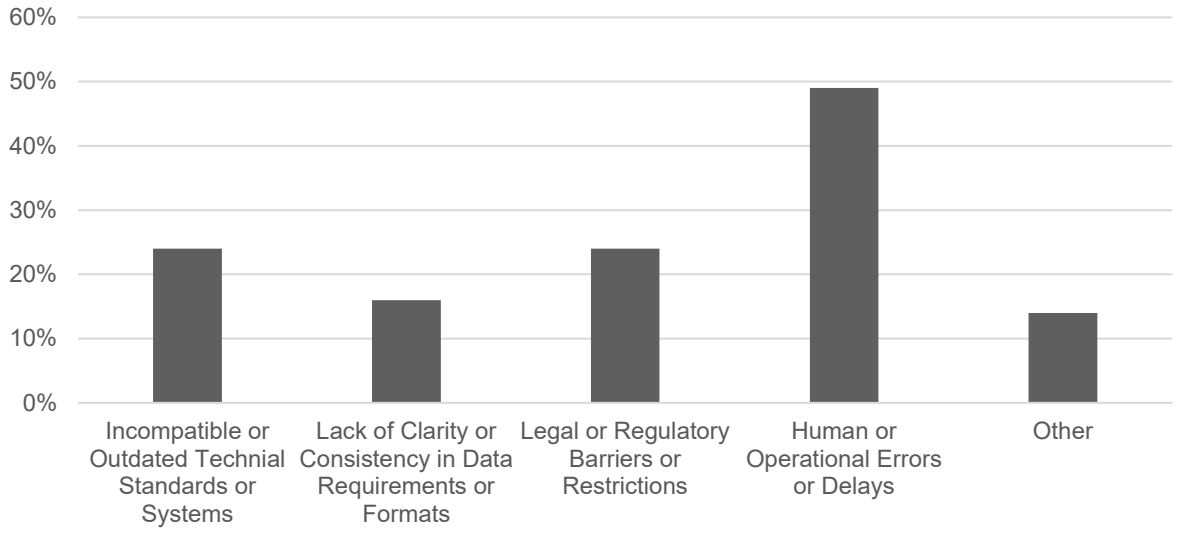
The survey results indicate that most UPU member countries have experienced challenges in handling data. Specifically, 69% of respondents have encountered difficulties, with 12% facing them frequently and 57% occasionally. This suggests that data protection issues are a common concern among the member countries, though the severity and frequency of these issues vary.

Figure 19 - Distribution of the Frequency of Difficulties or Challenges in Collecting, Processing, Transmitting or Receiving Data per Question 25



The most frequently cited issue, among 49% of the countries, is human or operational errors or delays. This suggests a significant impact of human factors on data protection efficacy, which could include a range of issues from lack of training to mismanagement of data protection protocols.

Figure 20 - Distribution of Main Causes or Sources of Difficulties or Challenges per Question 26



As outlined in recommendation A28, increased training can reduce the percentage of human or operational errors or delays. Nevertheless, it is understandable that human error is inevitable and cannot be reduced to zero.

The issue of legal or regulatory barriers or restrictions was cited by 24% of the respondents. As highlighted through the interviews, data protection levels among member countries are not uniform. While the GDPR is a strict regulation, it does offer several minimum best practices that can be met by other UPU member countries. Nevertheless, as not all member countries are subject to the GDPR nor seen by the EU as adequate third countries under Art. 46 of the GDPR, data transfers internationally can become burdensome.

24% of the responses cited technical standards or systems as a cause of difficulties. Hence, indicating a need for technological updates.

Recommendation A29: The PTC could analyze optimization possibilities concerning the technical environment among the member countries to reduce technical delays and fragmentations. Additionally, considering the importance of maintaining a secure postal network, it is recommended that the PTC expands its role to include conducting IT audits at the DOs. By conducting these audits, the PTC could identify vulnerabilities, strengthen security measures, and ensure a robust defense against potential threats, ultimately enhancing the overall integrity and reliability of the postal network.

16% of countries that reported a lack of clarity or consistency with data requirements or formats highlight the need for standardized data protection practices and clear guidelines that can be easily followed by all member countries. To ensure standardization and harmonization please refer to recommendation A2.

4. Data Collection and Protection Policies and Regulations in the International Postal Service

Designated operators collect and process a large volume of data for international postal processes. The core objective is to streamline the international exchange and delivery of mail and to be compliant with emerging requirements for the collection, processing and international transfer of data to ensure safe and efficient imports of international postal items.

For the purposes of providing international postal services, the following information is collected and/or generated:

- **Sender and Recipient Information:** Names and addresses of both the sender and the recipient are recorded.
- **Tracking Information:** Postal items are assigned a track and trace number, which allows for the monitoring of the item's journey.
- **Details on postal items:** Information regarding the contents of a postal items as well as information on the weight, value, and the number of items.
- **Customs and Import Data:** increasing amounts of data are collected to respond to the emerging requirements for the exchanged of electronic advance data (EAD) set for customs and security purposes. These requirements include, among other data, additional contact information of senders and recipients such as telephone numbers or email addresses. Since 2021, UPU Acts enforce the electronic advanced data exchange on all items containing goods exchanged between UPU member countries.

While some data elements, such as the track and trace number, may not constitute personal data on their own, their combination with other data may, in certain circumstances, result in the identification of a person. Conversely, certain data, like an individual's address, are inherently considered personal data.

The collection and processing of such data is crucial in the facilitation of international transfers of data between DOs and member countries, ensuring that postal items are processed and delivered with efficiency and security.

Exchanges of postal items between DOs have always involved the transmission of data, including personal data such as the names and addresses of senders and receivers. This information is a necessary requirement to ensure the efficient processing, transportation and delivery of (international) postal items to the addressee or to collect and send back those items, in the case of an unsuccessful delivery. Detailed procedures and regulations pertaining to the provision of postal services are contained in the UPU Acts that govern these exchanges.

The UPU can operate as both a data processor and a data controller, exemplified by its oversight and support of international mail exchange and control over customs-related data within its network. Furthermore, Article 133.5 of the UPU General Regulations explicitly mandates the International Bureau (IB) of the UPU to ensure the confidentiality and security of any commercial data provided by member countries and/or their designated operators for the performance of their obligations under the Acts of the Union.

As a data controller, the UPU is tasked with determining the processing purposes and methods for which personal data is processed. Concurrently, as a processor the UPU executes the processing of personal data based on the controller's instructions, which can be the DOs.

The interplay between these roles is essential in the management of data related challenges and opportunities and requires a comprehensive policy framework that addresses the complexities inherent in data collection and protection.

4.1. UPU Policy and Regulatory Framework

The mandatory UPU Acts, which includes the Constitution, the General Regulations, the Convention, and the Regulations to the Convention, contain specific obligations in terms of ensuring a single postal territory as well as the freedom of transit of postal items. These provisions relate to fundamental obligations and are part of international law. In addition, the UPU has established a comprehensive set of policies, guidelines, and agreements that give further effect to these obligations – including specific provisions relating to the collection and processing of data, including personal data.

As set out in the Constitution of the Universal Postal Union, member countries shall form, under the intergovernmental organization entitled the Universal Postal Union, a single postal territory for the reciprocal exchange of postal items. Freedom of transit shall be guaranteed throughout the entire territory of the Union, subject to the conditions specified in the Acts of the Union and any additional protocols thereto.

To give effect to the single postal territory and the freedom of transit, the UPU Acts provide for specific provisions regarding the exchange of postal items, which are specified in the Convention and Regulations to the Convention. The regulatory framework regarding the protection of personal data is based on several provisions set out in the Convention and the Regulations to the Convention, as well as the optional Postal Payment Services Agreement (PPSA), Postal Payment Services Regulations and the Multilateral Data Sharing Agreement (MDSA).

4.1.1. Universal Postal Convention

The Universal Postal Convention sets out the rules that give effect to the single postal territory of the Union and defines the basic, supplementary as well as optional postal services. The Universal Postal Convention also provides for the confidentiality of the data gathered by DOs and for the protection and security of that data. This Convention is binding on all member countries. It is critical that member countries ensure that the DOs fulfil the outlined obligations.

Provisions and Implications

The Convention provides a definition of personal data that, while it is not detailed, is intended to cover information necessary to identify a postal service user. This definition is broadly in line with current data protection regulations, which typically define personal data as any information relating to an identified or identifiable natural person.

Article 10(1) of the Convention mandates that personal data collected by DOs can only be used for the purposes for which they were originally collected. This aligns with the core principles of data minimization and purpose limitation found in many data protection laws and regulations, which seek to limit the processing of personal data to what is necessary in relation to the specific purposes stated at the time of collection and to prevent misuse.

Article 10(2) touches upon third-party disclosures and addresses the conditions under which personal data may be disclosed to third parties. It emphasizes that such disclosures are permissible only when authorized by the applicable national legislation. This clause, like existing data protection laws and regulations, attempts to reinforce the need for a legal basis or purpose for the personal data to be shared.

Article 10(3) obliges member countries and their DOs to ensure the confidentiality and security of users' personal data. This clause is a clear directive for the implementation of appropriate security measures to protect data against unauthorized access, disclosure, alteration, and destruction of such data, as in accordance with national legislations.

Article 10(4) focuses on the principle of transparency, requiring DOs to inform customers about the use of their personal data and the purposes for which it is collected. This is a fundamental aspect of data protection, as it empowers individuals by making them aware of how their data is being handled.

Article 10(5) addresses the transfer of personal data between designated operators of destination or transit countries. It states that designated operators may electronically transfer personal data to fulfill the service, provided that it is done without prejudice to the principles mentioned earlier in the article. This clause recognizes the need for data sharing between operators to facilitate the efficient delivery of postal services, while still upholding the principles of data protection and ensuring that such transfers are carried out in accordance with applicable national legislation.

Therefore, it is crucial that designated operators develop and implement clear policies, procedures and practices that are compliant with the UPU regulatory framework (see recommendations to develop and enhance data protection management programmes in Section 3 of this report). In order to enhance the universal understanding and coherent application of data protection practices among all member countries, the UPU should provide regular training and resources to the DOs on issues covered by the provisions of the Acts of the Union and MDSA.

Consequently, Article 10 of the Convention represents an effort to integrate important data protection principles into the international postal framework. It emphasizes purpose limitation, third-party disclosure restrictions, confidentiality, security, and transparency, which are all cornerstones of current data protection laws and regulations. However, the effectiveness of these provisions is contingent upon their implementation by member countries, which, in some cases, is subject to their national legislation.

Recommendation B1: Maintain the Convention provisions on processing of personal data, as they serve as cornerstones of current data protection laws and regulations. If the Convention is under review, it is recommended to consider broadening the existing provisions to encompass not only national obligations but also international obligations (like the PPSA). This would ensure that designated operators adhere to both domestic and international standards for data protection, fostering a comprehensive and globally harmonized approach to safeguarding personal data within the postal sector.

4.1.2. Postal Payment Services Agreement (PPSA)

The optional PPSA, currently with 72 Union member countries as parties, outlines that member countries and their DOs shall ensure the confidentiality and security of personal data in accordance with national legislation and international obligations. These provisions are critical in ensuring the protection of privacy and the secure handling of personal data within the postal payment services.

Provisions and Implications

Like the Convention, Article 9(1) of the PPSA imposes obligation on member countries and their DOs to ensure the confidentiality and security of personal data.

Article 9(2) of the PPSA outlines that the use of personal data is strictly limited to the purposes for which it was collected.

Both Article 9(1) and 9(2) of the PPSA further emphasize that these obligations must be adhered to in accordance with not only national legislation but also, where applicable, international obligations and the Regulations. By acknowledging the importance of complying with international obligations and the Regulations, the PPSA recognizes the need for a comprehensive approach that goes beyond national laws in safeguarding personal data.

Article 9(3) ensures that any sharing of personal data is justified and only permissible when authorized by applicable national legislation. This provision also serves as a safeguard against unauthorized disclosure, which could lead to privacy breaches and loss of trust.

Article 9(4) emphasizes the principle of transparency by requiring designated operators to inform their customers about the use and purpose for which their personal data has been gathered. This provision aims to empower individuals by providing them with clear and concise information about how their personal data will be utilized, ensuring transparency and promoting trust between the designated operators and their customers. By fulfilling this requirement, designated operators can enhance customer awareness and understanding of their data processing practices, fostering a more accountable and privacy-conscious approach to personal data management.

Article 9(5) requires that the data used to execute the postal payment order shall be confidential. Although not further outlined within this Article, the confidentiality requirement is in place to ensure that customers' financial details are protected from unauthorized access or disclosure.

The PPSA also includes the possibility for postal data (i.e. any data needed for the routing and tracking of a postal payment order or for statistical purposes, as well as for the centralized clearing system), to be shared with the IBonce a year for the purpose of quality of service, centralized clearing, and statistical purposes. However, Article 9(6) outlines that this data sharing is also subject to confidentiality.

The emphasis on confidentiality, purpose limitation, third-party disclosure, transparency, and secure data sharing reflects a commitment to safeguarding personal data within the postal payment services sector.

Recommendation B2: Maintain the PPSA provisions for data protection as they closely align with international best practices.

4.1.3. Multilateral Data Sharing Agreement (MDSA)

The MDSA was adopted to regulate the exchange of electronic data among postal sector entities of UPU member countries for the operation of international postal services. Although the Agreement is not binding on all UPU member countries, it requires its sixty signatories to ensure the physical and electronic security of the infrastructure and operating environment used for the exchange of data, with a view to preventing unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks, and to ensure the authenticity and integrity of the data. The MDSA aims to facilitate the operation of international postal services through the exchange of electronic data and underscores the importance of data security.

However, the MDSA's effectiveness is somewhat undermined by its voluntary nature and the lack of further detail on specific obligations. Not all UPU member countries have signed the agreement, which raises questions about its universal applicability and the consistency of data protection practices across the international postal network. The agreement's text could benefit from additional streamlining to enhance clarity and practicality, as it currently lacks a more comprehensive level of detail or guidance on certain topics as addressed below.

Definitions and principles

The UPU's approach to data protection through the MDSA is guided by several key definitions (like "Data Subject" and "Personal Data") and principles (like purpose limitation under Article 7(5) and confidentiality under Article 10) that align with international standards and best practices, including those outlined in the GDPR. While these definitions and principles are in line with international standards, it is important to note that they represent only a portion in relation to more comprehensive privacy regulations available worldwide.

Recommendation B3: To enhance clarity and consistency in the interpretation and application of the MDSA, it is recommended to expand and strengthen definitions to include a broader range of data protection and privacy concepts by incorporating common definitions from other relevant texts, including but not limited to the OECD Guidelines, the GDPR and SADC Model Law.

Furthermore, the MDSA currently lacks a clear definition of the roles of "controller", "processor" and "sub-processor". These roles play a crucial role in determining the responsibilities and obligations of different entities involved in data processing, and having a clear and universally understood definition is essential for ensuring proper implementation and compliance with privacy regulations. Without such clarity, there may be confusion and inconsistency in how these roles are interpreted and applied, potentially leading to gaps in data protection practices.

Recommendation B4: It is recommended to provide explicit definitions of the "controller". "processor" and "sub-processor" roles within the MDSA, taking into consideration commonly recognized definitions contained in other relevant texts, including but not limited to the OECD Guidelines, the GDPR and SADC Model Law.

By incorporating commonly recognized definitions and principles, the MDSA can effectively address the complexities of data protection within UPU member countries. This will contribute to alignment with international standards and promote a comprehensive and harmonized approach to data protection across member countries, ultimately enhancing the protection of personal data within the postal sector.

Recommendation B5: Enhance the existing data protection principles included in the MDSA and incorporate additional fundamental data protection and privacy principles, such as data minimization, purpose limitation, transparency, data security, and retention. These principles should reflect the relevant universal standards , allowing countries to agree upon them regardless of their legal framework.

The universal application of these data protection definitions and principles would promote a harmonized approach across UPU member countries, ensuring a consistent and uniform level of data protection.

Confidentiality and Security

The MDSA emphasizes the importance of confidentiality and security in the handling of personal data. This is a fundamental aspect of data protection, to ensure that personal data is not disclosed to unauthorized parties and to protect against any threats. The MDSA mandates the adoption of technical and organizational measures (TOMs) to safeguard data, although it only mentions these measures rather than providing a comprehensive guide on their implementation.

Recommendation B6: Introduce basic data protection measures focused on outcomes. Instead of providing a list of specific technical solutions that might be difficult to implement, MDSA should recommend general outcomes, such as “ensuring data is sufficiently protected against unauthorized access” and provide specific examples (like encryption, anonymization, etc.) without mandating them. Additionally, incorporate, to the extent possible, the basic requirements relating to protection of personal data by design and by default.

This flexibility and outcome-driven approach would allow countries to choose the most appropriate methods depending on their resources and capabilities.

Records of Processing Activities

The MDSA mentions the necessity of maintaining an up to date RoPA but it provides very limited guidance in terms of its scope and detail. A RoPA is a critical document that records all data processing

activities, serving as a tool for transparency and accountability. The lack of detailed guidance could lead to inconsistencies in how it is maintained.

Recommendation B7: Provide requirements within the MDSA regarding the scope and level of detail for a RoPA.

Rights Relating to Personal Data

The MDSA acknowledges the access right, setting a maximum period of seven calendar days for fulfilling such requests. However, the MDSA outlines this as a request coming from the parties to the MDSA, rather than from data subjects. Additionally, the MDSA does not elaborate on rights usually afforded to data subjects, such as the right to access, rectification or erasure, which are commonly recognized in comprehensive data protection regulations. It should, however, be recognized that the MDSA is an instrument of which purpose is to regulate the exchanges of electronic data between designated operators, including the protection of personal data as part of these exchanges, rather than providing rights to users of the postal services. Bearing in mind such a purpose and aim, the rights of data subjects may not be expressly covered in the MDSA. In any event, other relevant provisions, such as those concerning data retention, may be improved as outlined in the sections below, with a view to providing a better protection to data subjects.

Data Breach and Incident Responses

The MDSA addresses parties' commitment to assist in the identification and notification process of security breaches. However, it falls short in regulating or providing detailed guidance on the identification, handling, and reporting of such incidents. The lack of specificity could lead to inadequate responses to data breaches, potentially compromising rights, and security. A robust incident response plan as well as monitoring and reporting mechanisms for security breaches should be established. Routine testing is required to understand gaps in emergency plans and backup systems. These recommendations are further outlined in chapter 3.4.

Recommendation B8: Relevant principles regarding security incidents and data breaches may be incorporated in the MDSA to ensure a uniform understanding among member countries on such aspects. Such principles may also include basic data breach notification requirements.

Data Retention

The data retention periods that the MDSA offers depend on the applicable laws of the Receiving Party[15] and the purposes defined in Article 3. In cases where the Receiving Party's applicable laws do not specify a retention period, then the data shall be retained for a period which it deems reasonable for the associated purposes, but in any case, for a period no longer than 10 years from the date of receipt.

The data retention periods are broadly outlined in the MDSA and are based on the principle of purpose limitation and data minimization, meaning that the Receiving Party should only retain the data for as long as necessary. However, the MDSA refers to national laws and no additional clarification is provided on the deletion processes after the retention period has elapsed. This may create inconsistencies and uncertainties. As such, from a data protection perspective, the data retention periods that the MDSA offers may have some potential weaknesses, such as lack of clarity, transparency, and consistency

Recommendation B9: Set clearer guidelines on data retention periods, suggesting a review of the necessity of holding personal data periodically, with the possibility of shortening the maximum retention period from 10 years to a more reasonable timeframe where appropriate. Additionally, define deletion process to be followed after the retention period has elapsed.

[15] a Party that has received Data through Electronic data interchange from any other Party.

Further Considerations:

Responsible person (DPO)

There is no requirement for the appointment of a Data Protection Officer (DPO) or person responsible for data protection, and there is no requirement for the training of staff on data protection matters. Subject to availability of resources and without prejudice to the different needs of each stakeholder (depending on the scope and size of its operations), these may be seen as best practices to ensure a minimum level of awareness and execution of data protection principles.

Recommendation B10: To ensure awareness and execution of data protection principles, it is advisable to amend the MDSA with a view to including a strong recommendation for signatories to appoint a person or a team responsible for ensuring data protection compliance.

Accountability

The MDSA currently incorporates accountability principle by obligating parties to implement appropriate security measures, report breaches, and maintain data confidentiality. However, the existing provisions lack requirements for documentation or regular reviews of compliance efforts.

Recommendation B11: To enhance oversight and strengthen accountability, it is recommended to include provisions that emphasize the importance of documentation and regular assessments to ensure compliance with privacy practices. This should involve mandating parties to maintain records that demonstrate adherence to privacy practices, including implemented data protection measures and relevant policies or procedures. Additionally, it is advisable to establish a requirement for regular assessments, such as surveys and questionnaires, to evaluate the effectiveness of privacy practices and identify areas for improvement.

By enhancing the accountability principle in this manner, the MDSA can foster a culture of transparency, responsibility, and continuous improvement in data protection across member countries.

Cooperation

Cooperation within the MDSA is currently established through provisions that encourage parties to collaborate on matters related to data protection. However, there is a need to further promote cooperation by mandating parties to assist each other in fulfilling their obligations contained in the Acts of the Union and the MDSA regarding data protection.

Recommendation B12: To enhance cooperation, it is recommended to include provisions in the MDSA that require parties to actively support and assist one another in fulfilling their obligations contained in the Acts of the Union and the MDSA regarding data. This will foster a stronger collaborative environment and ensure a more effective implementation of data protection measures across member countries.

By promoting cooperation and mandating assistance among parties, the MDSA can establish a framework that encourages shared responsibility and collaboration, leading to improved data protection practices, streamlined processes, and enhanced trust among member countries.

Flexibility

An important feature of the MDSA is that it allows for flexibility to accommodate national regulations. This is crucial given the setup of the UPU but also the diverse legal landscapes of UPU member countries.

Recommendation B13: This flexibility of the MDSA should be maintained and continued with a robust baseline for data protection that all members can adhere to. The MDSA already allows for customization to accommodate regional or national requirements within the standardized framework of the MDSA, recognizing that different regions or countries may have unique data exchange needs and provide flexibility for adaptations that align with the core principles of the MDSA without compromising its overall effectiveness. [16] It is recommended that the relevant bodies of the UPU explore whether the possibilities (and flexibility) under the current MDSA may be further enhanced

In conclusion, while the UPU MDSA establishes a foundation for data protection within the postal sector, it exhibits several gaps and areas that require further development. Due to the lack of specificity and guidance on incident responses, data deletion and retention, the roles, and responsibilities, the MDSA could benefit from a more comprehensive approach. Nonetheless, its flexibility is a positive aspect that allows for the integration of the MDSA within different legal frameworks.

4.1.4. Other instruments

World Customs Organization – Universal Postal Union Postal Customs Guide

The World Customs Organization – Universal Postal Union (WCO–UPU) Postal Customs Guide is a joint tool that provides information and guidance for Designated Operators and Customs Administrations on the customs component of the postal supply chain. It aims to facilitate dialogue and coordination at a national level between the DOs of UPU member countries and Customs Administration. The guide also covers the relevant WCO standards, instruments, and tools, such as the Revised Kyoto Convention, the SAFE Framework of Standards, and the WCO Data Model.

Data protection is an important aspect of the postal customs clearance process, as personal data on users and information on the contents of postal items are collected, transmitted, and disclosed by DOs and Customs Administrations. The guide states that they shall respect the applicable national legislation on data protection and ensure the confidentiality and security of the data. The guide also advises designated operators to inform their customers of the use and purpose of their personal data and to obtain their authorization when necessary.

The guide also outlines the measures to enhance the security of the postal supply chain, such as the UPU security standards S58-3 and S59-3, the Authorized Economic Operator (AEO) status for DOs, the Pre-Loading Advance Cargo Information (PLACI) regime, and the Article 8 of the Convention on postal security. Considering the increased importance of security and of ensuring that DOs can continue to meet their customers' requirements, it is crucial that international security measures are implemented collectively and collaboratively, involving all stakeholders in the planning and decision-making stages. When establishing protocols and regulations related to the exchange of electronic postal data, it will be necessary to prioritize data security measures to prevent unauthorized entities from misusing or compromising the data, to safeguard individual privacy and protect proprietary business information. By that the trust of the public in the postal services offered by the DOs can be strengthened.

WCO-UPU Guidelines on Data Capture and Compliance with the CN 22/23

The WCO-UPU Guidelines on Data Capture and Compliance with CN 22/23 aim to provide practical guidance and best practices for DOs to capture and exchange electronic customs declaration data for postal items containing goods, in order to facilitate postal security and customs clearance.

[16] Annex 3 of the MDSA (region-specific annex) already allows for such a customization (see article 3.3 of the MDSA).

The CN 22 and CN 23 forms are customs declaration forms used for international postal shipments. They provide customs authorities with the necessary information to process packages, including the nature of the goods, their value, and their origin. Compliance with UPU guidelines for the CN 22 and CN 23 forms is mandatory for member countries and ensures a standardized approach to handling international mail, which facilitates trade and customs clearance.

The Guideline outline that to share data, data sharing agreements need to be in place and consider the issues of data sharing between DOs but also between DOs and customs administrations.

WCO-UPU Guidelines on the Exchange of Electronic Advance Data between Designated Operators and Customs Administrations

The Guidelines provide an overview of the benefits and challenges of exchanging EAD between DOs and customs administrations in the context of postal security and e-commerce.
From a data protection and privacy perspective, the Guideline highlight the importance and diversity of data privacy and protection legislations that apply to the exchange of EAD, which may include personal data of senders and addresses.

The Guideline cover the technical aspects of EAD transmission, such as the data quality and data standards to ensure the accuracy and completeness of the data. Therein continuing the sentiments that DOs should address the data protection aspects of data sharing, be it the purpose, scope, and security of data.

Revised Kyoto Convention

While the Kyoto Convention, a multilateral agreement on the harmonization of customs procedures, is not per se part of the UPU's legal framework, it also needs to be mentioned here, since it includes provisions that directly impact the handling and data protection within the customs process and thereby influence the UPU's legal framework concerning data protection. The Kyoto Convention acknowledges the importance of an open and collaborative exchange of information, but stipulates that any information must be treated as confidential and limited to the purposes for which it was shared. The Convention indicates some data protection approaches but is not as comprehensive as the MDSA.

4.2. Data Processing within the UPU

The UPU has a 27001 ISO certification for the main postal services, covering the network system, the big data infrastructure and cloud solutions. Through the ISO 27701 certification process, it has also been identified which personal data is being processed and it is intended to seek certification for this towards the end of 2025. The preparation work conducted in 2024 towards this certification, led to qualifying the UPU as a data processor.

In cases concerning internal audits conducted by DOs, questions have been raised about how to handle personal data when exchanging information for international mail. Although these requests can be time intensive, guidance on how to process such data and comply with obligations to operate in a controlled environment and in a controlled manner is provided within the UPU.

With regard to documentation and responding to requests, and for preparing for the ISO 27701 certification, a RoPA has been created which seems to follow generally adopted data protection standards and principles. The RoPA has been well perceived and does not present any challenges. Although no data subject requests have yet been addressed to the UPU directly, processes were put in place to efficiently accommodate requests from data subjects. Additionally, mechanisms for member countries to transparently report data breaches or security incidents are also provided. Some recent experience shows that the DOs are increasingly exposed to cyber-attacks that potentially impact the UPU's PTC systems. This can be the case when local systems are not adequately managed (e.g.,

insufficient backups, insufficient patches). Such instances further advocate for the use of the cloud and the PTC solutions that are available.

The interview has highlighted that there has been significant collaboration with DOs to increase awareness and distribute best practices. Such collaboration will continue to be essential in shaping data protection within the UPU.

4.3. Data Collection and Processing for the purposes of postal security and customs clearance

As the UPU endeavors to modernize postal products and services, it is imperative to harmonize processes and uphold uniform standards of data protection. The following contextual insights highlight the challenges currently faced in regard to data collection and processing for the purposes of postal security and the clearance of postal items by customs authorities. The exchange of electronic advance data (EAD) is fundamental to ensuring the appropriate security and customs conditions for the dispatch of international postal items. For instance, the sharing of EAD assists the prevention and prosecution of illegal use of the postal network to deliver dangerous and/or illegal items, such as narcotics or counterfeit drugs, as well as other dangerous items, such as explosives.

With regard to international transfers, where DOs' operations require the transfer of personal data, several multi- or bilateral agreements can be agreed on to facilitate the transfer of EAD. However, the several agreements to facilitate the transfer of personal data showcase an administrative burden and highlight the fact that the MDSA is not mandatory to all member countries. With the number of possible agreements, a level of confusion exists as several requirements and agreements need to be continuously met.

EAD requirements are included in the customs declaration and are a clearly defined data set. To process and receive such data, some DOs use their own bespoke systems developed by IT providers while other operators use the PTC services. The PTC, where it processes the data, does so in accordance with the ISO standards and with data centers based in Switzerland. Where DOs share data, data sharing agreements are signed, but the processing must be done according to their own legislation and that of the other DOs. As aforementioned, this can lead to a wide range of obligations needing to be met.

Additional challenges are faced by some of the developing countries where the power supply is unreliable and can interrupt their data transmission and processing. They depend on PTC tools to facilitate their data collection, but they also need to ensure that they have backup power or alternative methods in case of outages.

Data quality is a major challenge and a key factor for the success of the EAD. Consistent with data protection principles (see section 2), the adequacy, accuracy and completeness of (personal) data is critical, including such information provided in declarations for the purposes of security and processing of postal items by customs authorities. However, this issue is on the UPU's radar, and measures have been put into action to provide the appropriate tools and education to DOs and explain to customers what data is relevant and important.

Electronic Advance Data (EAD)

UPU member countries and their DOs are required to observe the security requirements as defined in the Acts and as implemented through the relevant standards and frameworks that give effect to those requirements. The exchange of EAD is critical for the safe and secure exchange, including the transport and transit operations, of postal items between DOs and other relevant postal supply chain stakeholders. In response to emerging security requirements, the UPU has adopted or is currently considering the adoption, within its regulatory framework, of rules aimed at ensuring the provision of relevant data to certain eligible stakeholders, such as national authorities responsible for security and customs processing, with a view of identifying potential high-risk postal items travelling through the global postal network. It was previously mentioned that such data, such as the official UPU customs declaration forms (CN 22 and 23) contain personal data, including the names and addresses of the sending and receiving users of the postal service.

The different forms, and the equivalent electronic message standards, have been developed in coordination with or acknowledged by various international organizations, including the World Customs Organization (WCO), the International Air Transport Association (IATA) and the International Civil Aviation Organization (ICAO).

Nevertheless, ensuring data quality is an integral foundation to the subsequent processing and efficiency of the postal service.

4.4. Nexus between UPU Acts and Internal (and Regional) Laws and Policies on data protection

The processing of personal data is already regulated by various member countries and their data protection regimes and policies. The introduction of new data protection regulations and laws, including the GDPR in particular created a reinforced framework that caused DOs to review their practice and compliance. It also created an increased awareness on the part of the data subjects. This resulted in a number of amendments to the processes applicable to postal services, without fundamentally impacting the activity of postal services *per se*. The introduction of such regulations and laws also had a profound impact on the potential consequences of non-compliance – and awareness thereof.

Notwithstanding the above, UPU member countries and their designated operators, are bound by treaty obligations that require them to ensure a single postal territory, which includes the collection and processing of personal data required to fulfil the obligations as set out in the UPU Acts. These fundamental principles of the Union are consistent with the acknowledgment of postal services as essential services to citizens in the exercise their freedom of expression and information as provided for by Article 19 of the International Covenant on Civil and Political Rights.[17]
The UPU Acts furthermore require, on a mandatory basis, the exchange of personal data through standardized forms and messages, the application and use of barcodes (for example for the purposes of interfacing with supply chain stakeholders) as well as the use of tracking information.

The GDPR, in particular, contains specific provisions for such international transfers. With these provisions, the GDPR aims to guarantee that personal data transferred outside of the EU is subject to an equivalent level of protection to that applied within the EU. In its judgment C-311/18 (Schrems II), the European Court of Justice (ECJ) stated that controllers and processors of personal data, acting as exporters of such data are in fact responsible for verifying, on a case-by-case basis, whether the laws and practices of the third country impinge on the effectiveness of the safeguards provided for in Article 46 of the GDPR (i.e. transfer tools). In this regard, that judgment, like any other domestic or regional court decisions, shall not release UPU member countries (and their designated operators) from their treaty-based obligations as set forth in the Acts of the Union. It is, furthermore, impractical for each designated operator to assess the legal framework of all 192 UPU member countries – especially when recognizing that the European Commission considers that only 11 countries provide for adequate protection of personal data.[18]

Research and interviews identified various points of friction inherent to the structure of an international body, governed by international law, and including member countries that must comply with their own specific regulations. This is particularly the case for international postal delivery, where DOs may feel they are operating in a grey area between, on the one hand, the legitimate interests of the collection, processing and international transfer of personal data in the public interest of fulfilling binding international treaty-based obligations and ensuring a universal postal service and, on the other hand, the restrictions that the same DOs may deem as being imposed by domestic and/or regional frameworks (as may be the case with the GDPR and the transfer of postal data outside of the European Economic Area (EEA)), with the consequent application of fines for the violation of data protection

[17] It should be noted the relationship between Article 17 and 19 of the former of which provides that “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”.
[18] The European Commission has so far (July 2024) recognised Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom (under the GDPR and the LED), the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay as providing adequate protection.

regulation.[19] The confusion that these various obligations create and the relationship between these different legal instruments need to be clarified. The following principles give guidance in terms of how the relationship should be understood:

- The UPU Acts are binding upon all Union member countries and must be complied with in good faith. Domestic and/or regional frameworks (including the GDPR), like any internal or regional regulation, do not release UPU member countries and their designated operators, including those of the EEA, from their obligation to fully comply with the provisions of the UPU Acts.

- It should be recognized that there is a significant degree of continuity of the main principles of EU data protection legislation in force before the GDPR, in particular the 1995 EU Data Protection Directive. While the underlying principles are the same, postal services were not affected by the restrictions that applied before the GDPR came into effect.
- Furthermore, international treaty-based obligations provide for the necessary legal basis for the processing of personal data. The concept of 'necessity' is a key element in the context of 'compliance with a legal obligation', as the data processing must be actually *necessary* in order to comply with the obligation. Other legal bases for the processing of data may also include, *inter alia*, a contract or, as referred to in Article 10 of the Convention, the provisions of national laws.
- Certain domestic and/or regional frameworks, such as the GDPR, provide for "appropriate safeguards", such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). Where applicable, the UPU Multilateral Data Sharing Agreement could be considered a relevant transfer tool as it contains provisions and elements towards implementing data protection principles relevant to the international transfer of data.

The abovementioned principles are inter-related and should be considered together.

In what specifically pertains to domestic and regional regulatory initiatives (including without limitation the GDPR), a formal dialogue between the UPU and relevant domestic and/or regional authorities could be seen as beneficial for achieving better identification and, as appropriate, harmonization of the practices in place, while at the same time ensuring due respect of (i) the public international law commitments assumed by UPU member countries under the Acts and (ii) the specific status of the UPU as an intergovernmental organization and specialized agency of the United Nations. For example, work could be conducted to draft harmonized standard clauses and clearer processes for international data transfers.

In the context of international postal service, personal data has tended to be minimized. For most cases, the personal data exchanged is minimal as it contains only the data necessary for the performance of the postal service (commonly the name and contact details of senders and recipients, including the addresses). Other instances may present different questions of a more sensitive nature or interpretation of personal data, such as signatures upon delivery. For all questions pertaining to such a nature, the focus is on the risk of harm to the data subject.

Without prejudice to the relationship between international law (treaty-based obligations under the UPU Acts) and internal law, of which the former mandates the collection, processing and exchange of personal data, one of the biggest concerns that DOs may face concerns the process of submitting standard contractual clauses to the review and acceptance of the relevant data protection supervisory authorities. While efforts are made to align with concepts introduced by certain domestic and/or regional frameworks (such as the GDPR), not every version satisfies those requirements. In practical terms, ssuch frameworks have led to a situation that it leaves little or no room for alternatives, forcing DOs either to unilaterally adhere to such conditions, or cause them to operate in an allegedly non-compliant manner.

[19] The monitoring and enforcement of the GDPR in the specific circumstances of each case fall within the competences of the (national) data protection supervisory authorities.

Outside of such domestic and/or regional frameworks, other challenges have been faced, mainly the risk of mis-delivery being qualified as a data breach by some member countries authorities and the risk of cyber-attacks and consequences from a data protection standpoint.

With respect to the data subject requests, these requests are typically addressed to DOs, without any challenge other than a sometimes pre-conceived notion that the right to deletion is absolute. As these rights have not been clarified nor frequently requested, this is not as much of a debated topic, however, processes are in place to address such requests.

Some improvements could be implemented by ensuring a common level of transparency, translating into clear, harmonized privacy notices, explaining clearly which type of data is collected, how it is processed and with whom it is shared. As an example, a recommended practice encountered was the proper mapping of data and its processing, which proved helpful to understand how personal data is handled, identify the associated risks and prioritize adequate mitigation measures. Both these measures could be designed and promoted to the member countries to ensure better compliance with data protection principles.

4.5. Standards and Compliance

Within the UPU, general compliance is being monitored from both a legal perspective and a technological perspective.

Currently, personal data is stored and managed from several central databases, where TOMs are applied such as encryption and access control. However, when reviews are initiated on these databases some of the personal data is missing that impacts the data quality, such as missing addresses or phone numbers. Currently the reviews are conducted at a relatively high level and not further checked than the region and zip code, for example. However, to ensure data quality and accuracy it should be possible to also check that the street name is correct. Nevertheless, this is a known issue, however, due to the volume of data and other priorities regarding the data set, and not yet being fully digital, this has not yet been conducted. There is currently a regional approach to push the posts to improve the data quality.
Overall, from the discussions surrounding the database, it illustrates that among the member countries and DOs there may be a mismatch on the broad data protection principles and obligations that the members must adhere to. However, there are discussions regarding how to improve the data quality, for example through remuneration measures.

Conclusions

The international postal service is carried out in a diverse regulatory environment, where different countries may have different data protection laws, regulations, and requirements, such as the EU-enacted GDPR. Treaty-based obligations require member countries and their DOs to fulfil the mandatory postal services set out in the UPU Acts. The UPU legal instruments include various provisions relating to data protection and international transfers and provide for a legal basis to perform international postal services. Under certain domestic or regional legal systems, the collection, processing and transferring for the purposes of performing those services may need to be proportionate and needs to adhere, to the extent possible, to the various data protection principles and data subject rights as provided for under such legal systems. Where personal data is collected, transferred, and processed, the DOs shall ensure that they respect the data protection principles set out in the Convention and its Regulations, as well as, where applicable, in the PPSA, its Regulations and the MDSA. On an ongoing basis, the UPU needs to review its data protection framework to ensure that adequate safeguards and guarantees for the protection of the personal data.

5. Recommendations

5.1. Best practices and recommendations

The following table serves as a distillation of the best practices and strategic recommendations made in sections 2, 3 and 4 of this study. Group A recommendations are those covered in section 3 concerning the development of an effective data protection management programme based on best practices. Group B recommendations are those covered in section 4 concerning the further improvement and development of the various legal instruments of the UPU's own policy and regulatory framework.

5.1.1. Recommendations for an effective data protection management programme

Table 1: Group A recommendations relevant to the development and implementation of a data protection management programme (recommendations as provided in section 3).

Reference	**Identified Best Practice**	**Recommendations**
A1 (Data Protection Management Programme)	Foster a centralized forum for member countries to discuss, and adopt standardized data protection practices, ensuring a baseline of privacy and security across the international postal services.	To effectively navigate the complexities within the regulatory landscapes, the UPU should play a role in facilitating discussions to establish best practices and lessons learned in the area of data protection. This could be done by various means, such as organizing workshops, best practice seminars, or dedicated sessions within the existing platforms like the Conference on Postal Regulation or the Postal Regulatory Forum, specifically focused on data protection. This collaborative approach will enable the identification of common trends, emerging issues, and effective solutions that can be implemented across the postal sector. Alternatively, the UPU could consider establishing a task force with a clear mandate to develop uniform data protection practices and strategies. This task force would bring together experts from member countries to collaborate on the creation of comprehensive guidelines and frameworks that promote consistent and effective data protection measures.
A2 (Data Protection Management Programme)	Establish a common framework that aligns with the baseline standards of privacy regulations.	The UPU should adopt a harmonized and common approach to data protection based on fundamental principles of data protection.
A3 (Data Protection Management Programme)	Regular data protection training.	The establishment and fostering of shared knowledge, guidance, training, and supplementary material is essential to cultivate a common understanding of data protection. Please also refer to recommendations A10, A14 and A28.
A4 (Data Protection Management Programme)	Improve understanding and communication of the benefits of the MDSA while respecting and operating within the framework of each member country's national commitments and legal obligations.	As indicated in UPU Policy and Regulatory Framework , it is recommended that the UPU takes proactive measures to encourage more of its member countries to become signatories to the MDSA, promoting harmonized adherence to best practices within the realm of data protection. To achieve this, it is suggested to discuss and collaborate with member countries to better understand their concrete reasons for not signing and address any potential hesitations they may have.

A5 (Data Protection Management Programme)	Assign clear roles and responsibilities.	For those member countries without a person or team responsible for ensuring data protection compliance, it is recommended to establish such a function. This will ensure a clear point of communication and responsibility for all data protection matters. The existing language used in the MDSA does not mandate the appointment of a DPO or an equivalent role. However, adhering to best practices would strongly suggest designating an individual to oversee data protection responsibilities and compliance. It is advisable to amend the MDSA to include this requirement.
A6 (Data Protection Management Programme)	Foster a culture of open communication and collaboration.	For those already with dedicated data protection teams or DPOs, the sharing of best practices and experiences amongst the member countries will support in developing harmonized strategies and lessons learned.
A7 (Data Protection Management Programme)	Provide clear, concise, and accessible privacy notices to fulfill transparency obligations.	It is recommended to clearly communicate with postal service users how their personal data is being processed and the safeguards in place for data protection. This can be done in the form of a privacy notice.
A8 (Data Protection Management Programme)	Conduct assessments to identify both strengths and areas for improvement.	It is recommended to assess data protection practices on a regular basis to identify areas for improvement and determine what is effective.
A9 (Data Protection Management Programme)	Creating commonly accepted guidelines for privacy notices and terms and conditions.	To unify information obligations, the UPU could create guidelines for privacy notices and terms and conditions, that would be customizable to the specific needs of the postal sector.
A10 (Data Protection Management Programme)	Regular data protection training.	To enhance the universal understanding of data protection practices among all member countries, the UPU should offer training and resources to DOs, particularly in the developing regions, through workshops and webinars regarding the data protection requirements in the Convention. Please also refer to recommendations A3, A14 and A28.
A11 (Data Protection Management Programme)	Conduct assessments to ensure member countries' compliance.	A monitoring mechanism should be in place to ensure that all member countries are adhering to their information and data protection obligations and are updating their information instruments regularly. This could involve regular surveys, audits, or peer reviews.
A12 (Data Protection Management Programme)	Regular reviews of data protection policies to ensure ongoing compliance.	All member countries should be encouraged to regularly review and update their privacy policies and consent forms. This should be done not only in response to changes in data processing activities but also to reflect changes in the legal and regulatory landscape.
A13 (Data Protection Management Programme)	Establish clear policies and procedures within the data governance framework.	To ensure compliance with Art. 10(1) of the UPU Convention, which outlines the purpose limitation for data processing, it is crucial to develop and implement systematic processes to ensure data is used only for its intended purposes.

A14 (Data Protection Management Programme)	Regular data protection training.	Implement and foster continuous data protection training programs specially focusing on improving the confidentiality and security of data exchanges. Please also refer to recommendations A3, A10 and A28.
A15 (Data Protection Management Programme)	Establish clear policies and procedures within the data governance framework.	All member countries should be encouraged to develop comprehensive written policies and procedures pertaining to roles and responsibilities. These documents should be regularly reviewed and updated to reflect current best practices and legal requirements.
A16 (Data Protection Management Programme)	Regularly update systems to protect against technical vulnerabilities.	Continual investment in and updating of technical measures are crucial as threats evolve. For those not using these measures, action is recommended to implement robust technical defenses.
A17 (Data Protection Management Programme)	Data Protection Governance and Strategy.	All member countries must have a data protection strategy.
A18 (Data Protection Management Programme)	Routine testing schedule for emergency plans and backup systems.	Immediate action is required to address and understand the gaps in emergency plans and backup systems to ensure adherence to the MDSA and preparedness against potential outages.
A19 (Data Protection Management Programme)	Establish a robust incident response plan.	All countries responding that they do not monitor or report security incidents, especially for those subject to the MDSA, should take immediate action to establish a monitoring and reporting mechanism for security breaches relating to personal data.
A20 (Data Protection Management Programme)	Assign clear roles and responsibilities.	All member countries should adopt a policy to outline who needs to be notified in case of security incidents and data breaches.
A21 (Data Protection Management Programme)	Establish clear and specific definitions.	It is recommended to enhance clarity regarding the definition of security incidents or data breaches to potentially improve response times.
A22 (Data Protection Management Programme)	Establish appropriate timeframes.	As a best practice, establish a plan and timeframe for regular security assessments as part of an overarching security assessment policy.
A23 (Data Protection Management Programme)	Establish appropriate retention schedules.	It is critical to establish high-level clear retention schedules that do not supersede national and international requirements but outline best practices for those who do not have the necessary guidance from national legislation.
A24 (Data Protection Management Programme)	Outline appropriate procedures for the disposing of personal data.	Clear guidelines and policies should be created on the proper disposal and deletion of no longer needed personal data to comply with the principles of data minimization.
A25 (Data Protection Management Programme)	Enable and clarify data subject rights.	In developing regions, it is important to foster a minimal level of data subject rights which can be attained.
A26 (Data Protection Management Programme)	Enable and clarify data subject rights.	The UPU should promote the establishment of formal policies. This should include clear guidelines on how to respond to different types of requests, who is responsible

		for responding, what to document, and within what timeframe.
A27 (Data Protection Management Programme)	Creating commonly accepted guidelines for RoPA.	It is recommended that the UPU support its member countries by providing comprehensive guidelines on the RoPA. These guidelines should outline the obligatory pieces of information required for completion and include examples for ease of understanding. By doing so, the UPU can ensure a certain level of standardization across postal services and promote the harmonization of data protection practices in the postal sector. Additionally, it is suggested that internal guidelines be established for the frequency of reviewing and updating the RoPA, with an annual review being the commonly accepted minimum.
A28 (Data Protection Management Programme)	Regular data protection training.	The availability of regular training can be promoted by the UPU to accelerate and ease access to data protection best practices. Please also refer to recommendations A3, A10 and A14.
A29 (Data Protection Management Programme)	Technological optimization.	The PTC could analyze optimization possibilities concerning the technical environment among the member countries to reduce technical delays and fragmentations. Additionally, considering the importance of maintaining a secure postal network, it is recommended that the PTC expands its role to include conducting IT audits at the designated operators (DOs). By conducting these audits, the PTC could identify vulnerabilities, strengthen security measures, and ensure a robust defense against potential threats, ultimately enhancing the overall integrity and reliability of the postal network.

5.1.2. Recommendations for the further development of the UPU Policy and Regulatory Framework on data protection

Table 2: Group B recommendations relevant to the various policies and legal instruments (recommendations as provided in section 4).

Reference	**Policy and legal instrument**	**Recommendations**
B1 (Policies and Frameworks)	Maintain Convention provisions.	Maintain the Convention provisions on processing of personal data, as they serve as cornerstones of current data protection laws and regulations. If the Convention is under review, it is recommended to consider broadening the existing provisions to encompass not only national obligations but also international obligations (like the PPSA). This would ensure that designated operators adhere to both domestic and international standards for data protection, fostering a comprehensive and globally harmonized approach to safeguarding personal data within the postal sector.
B2 (Policies and Frameworks)	Maintain PPSA provisions.	Maintain the PPSA provisions for data protection as they closely align with international best practices.
B3 (Policies and Frameworks)	Expand and strengthen definitions in the MDSA.	To enhance clarity and consistency in the interpretation and application of the MDSA, it is recommended to expand

		and strengthen definitions to include a broader range of data protection and privacy concepts by incorporating common definitions from other relevant texts, including but not limited to the OECD Guidelines, the GDPR and SADC Model Law.
B4 (Policies and Frameworks)	Clearly defines parties' roles within the MDSA.	It is recommended to provide explicit definitions of the "controller", "processor" and "sub-processor" roles within the MDSA, taking into consideration commonly recognized definitions contained in other relevant texts, including but not limited to the OECD Guidelines, the GDPR and SADC Model Law.
B5 (Policies and Frameworks)	Incorporate basic privacy principles in the MDSA.	Enhance the existing data protection principles included in the MDSA and incorporate additional fundamental data protection and privacy principles, such as data minimization, purpose limitation, transparency, data security, and retention. These principles should reflect the relevant standards, allowing countries to agree upon them regardless of their legal framework.
B6 (Policies and Frameworks)	Introduce basic data protection measures focused on outcomes in the MDSA.	Introduce basic data protection measures focused on outcomes. Instead of providing a list of specific technical solutions that might be difficult to implement, MDSA should recommend general outcomes, such as "ensuring data is sufficiently protected against unauthorized access" and similar provide specific examples (like encryption, anonymization, etc.) without mandating them. Additionally, incorporate, to the extent possible, the basic requirements relating to protection of personal data by design and by default.
B7 (Policies and Frameworks)	Provide requirements for RoPA within the MDSA.	Provide requirements within the MDSA regarding the scope and level of detail for a RoPA.
B8 (Policies and Frameworks)	Introduce the relevant principles regarding security incidents and data breach, including basic notification requirements in the MDSA.	Relevant principles regarding security incidents and data breaches may be incorporated in the MDSA to ensure a uniform understanding among member countries on such aspects. Such principles may also include basic data breach notification requirements.
B9 (Policies and Frameworks)	Set clearer data retention guidelines within the MDSA.	Set clearer guidelines on data retention periods, suggesting a review of the necessity of holding personal data periodically, with the possibility of shortening the maximum retention period from 10 years to a more reasonable timeframe where appropriate. Additionally, define deletion process to be followed after the retention period has elapsed.
B10 (Policies and Frameworks)	Include in the MDSA a strong recommendation for signatories to appoint a person or a team responsible for ensuring data protection compliance.	To ensure awareness and execution of data protection principles, it is advisable to amend the MDSA, with a view to including a strong recommendation for signatories to appoint a person or a team responsible for ensuring data protection compliance.

B11 (Policies and Frameworks)	Add provisions enhancing accountability.	To enhance oversight and strengthen accountability, it is recommended to include provisions that emphasize the importance of documentation and regular assessments to ensure compliance with privacy practices. This should involve mandating parties to maintain records that demonstrate adherence to privacy practices, including implemented data protection measures and relevant policies or procedures. Additionally, it is advisable to establish a requirement for regular assessments, such as surveys and questionnaires, to evaluate the effectiveness of privacy practices and identify areas for improvement.
B12 (Policies and Frameworks)	Include provisions that require parties to actively support and assist one another in fulfilling their obligations towards data protection.	To enhance cooperation, it is recommended to include provisions in the MDSA that require parties to actively support and assist one another in fulfilling their obligations contained in the Acts of the Union and the MDSA regarding data protection. This will foster a stronger collaborative environment and ensure a more effective implementation of data protection measures across member countries.
B13 (Policies and Frameworks)	MDSA flexibility.	The flexibility of the MDSA should be maintained and continued with a robust baseline for data protection that all members can adhere to. The MDSA already allows for customization to accommodate regional or national requirements within the standardized framework of the MDSA, recognizing that different regions or countries may have unique data exchange needs and provide flexibility for adaptations that align with the core principles of the MDSA without compromising its overall effectiveness. It is recommended that the relevant bodies of the UPU explore whether the possibilities (and flexibility) under the current MDSA may be further enhanced

5.2. Practical implementation and evaluation of the recommendations

This section offers a practical examination of the proposed recommendations, detailing the steps for implementation and considerations for the UPU to deliberate on. The recommendations provided here below are the same as those outlined in section 5.1 and 5.2 but provided in more detail as they furthermore include a high-level roadmap towards their practical implementation.

5.2.1. Practical implementation of recommendations an effective data protection management programme

Recommendation A1

To effectively navigate the complexities within the regulatory landscapes, the UPU should play a role in facilitating discussions to establish best practices and lessons learned in the area of data protection. This could be done by various means, such as organizing workshops, best practice seminars, or dedicated sessions within the existing platforms like the Conference on Postal Regulation or the Postal Regulatory Forum, specifically focused on data protection. This collaborative approach will enable the identification of common trends, emerging issues, and effective solutions that can be implemented across the postal sector. Alternatively, the

UPU could consider establishing a task force with a clear mandate to develop uniform data protection practices and strategies. This task force would bring together experts from member countries to collaborate on the creation of comprehensive guidelines and frameworks that promote consistent and effective data protection measures.

Practical Implementation: A data protection checklist, encompassing the widely recognized best practices, can serve as a valuable benchmark for member countries to evaluate their existing data protection practices against. By cross-referencing their current measures with those outlined in the checklist, member countries can confidently ascertain whether their practices are in alignment with the UPU stipulated best practices.

Recommendation A2

The UPU should adopt a harmonized and common approach to data protection based on fundamental principles of data protection.

Practical Implementation: To achieve a level of uniformity among the member countries of the UPU, it is proposed that the existing instruments should integrate fundamental data protection standards that reflect an achievable level of best practices observed globally. Introducing these principles into the MDSA would align the disparate data protection legislations of the member countries, fostering a more cohesive approach to data protection.

Recommendation A3

The establishment and fostering of shared knowledge, guidance, training, and supplementary material is essential to cultivate a common understanding of data protection.

Practical Implementation: To foster appropriate awareness of data protection principles and practices, it is highly recommended to create a readily available database with all the training material that can be continuously referred to.

The UPU should develop comprehensive training modules that cover various aspects of data protection, including legal frameworks from the UPU, including the Convention and the MDSA. This can be done as quarterly webinars, online modules, regional workshops, or alternative training sessions and is followed by all member countries. This should also foster collaboration and open discussions about what works well in practice and what can be improved or further worked on. To ensure the training has a lasting impact, the UPU could introduce a certification process for those who complete and maintain the training.

Additionally, the UPU can establish a schedule for regular updates and refresher courses to keep member countries abreast of the latest developments and best practices in data protection. Therein, the UPU can encourage member countries to share their experiences and resources, further fostering a collective understanding of data protection.

Recommendation A4

As indicated in UPU Policy and Regulatory Framework , it is recommended that the UPU takes proactive measures to encourage more of its member countries to become signatories to the MDSA, promoting harmonized adherence to best practices within data protection. To achieve this, it is suggested to discuss and collaborate with member countries to better understand their concrete reasons for not signing and address any potential hesitations they may have.

Practical Implementation: Initiatives could include providing support and resources to help countries better understand the MDSA and therein demonstrating the value of a common level unified baseline approach to data protection. Raising awareness through similar means as outlined in recommendation 3, to share the benefits of signing the MDSA and its overall goals, the MDSA FAQs can be further elaborated on to support this recommendation.

Recommendation A5

For those member countries without a person or team responsible for ensuring data protection compliance, it is recommended to establish such a function. This will ensure a clear point of communication and responsibility for all data protection matters.

The existing language used in the MDSA does not mandate the appointment of a DPO or an equivalent role. However, adhering to best practices would strongly suggest designating an individual to oversee data protection responsibilities and compliance. It is advisable to amend the MDSA to include this requirement.

Practical Implementation: The UPU could call for the establishment of a dedicated DPO role or responsible person within the member countries respective postal administrations. This role or team would be tasked with developing and overseeing a comprehensive data protection strategy, ensuring compliance with relevant laws, and serving as the primary contact for data privacy inquiries and issues. It aligns with global trends towards strengthening data privacy and would centralize responsibility, enhancing the member countries' ability to adhere to data protection regulations.

Recommendation A6

For those already with dedicated data protection teams or DPOs, the sharing of best practices and experiences amongst the member countries will support in developing harmonized strategies and lessons learned.

Practical Implementation: The UPU could establish a forum or secure online platform where member countries' data protection teams and DPOs can exchange information, strategies, and case studies. Additionally, the UPU could organize regular webinars or workshops for these responsible persons with a focus on key data protection topics, encouraging the sharing of insights across member countries and improving general exchange among member countries.

Recommendation A7

It is recommended to clearly communicate with postal service users how their personal data is being processed and the safeguards in place for data protection. This can be done in the form of a privacy notice.

Practical Implementation: The UPU could develop guidelines for privacy notices that reflect international data protection best practices and demand the member countries to adopt and customize it for their domestic postal services. These guidelines could be made available in multiple languages and include clear guidelines on how to communicate the purposes of the processing of personal data and the safeguards in place to protect personal data. Member countries could then be mandated to prominently display this privacy notice at all postal service points and on their official websites.

Recommendation A8

It is recommended to assess data protection practices on a regular basis to identify areas for improvement and determine what is effective.

Practical Implementation: The UPU could develop a standardized data protection assessment framework, therein establishing and monitoring auditing practices through regular gap assessments. This is a critical step towards ensuring that data protection standards are set and effectively adhered to. Regular gap assessments can help identify areas where data protection practices are lacking or could be improved.

The first step is to create a comprehensive framework for assessing the current state of data protection practices. This should include the main principles contained within the Convention and its Regulations. Furthermore, a regular schedule is needed to ensure a consistent approach to monitoring data protection practices.

After each assessment, the findings should be documented and reported to the relevant stakeholders. Based on these findings, it is essential to jointly develop action plans to rectify identified gaps, ensuring their timely implementation.

Recommendation A9

To unify information obligations, the UPU could guidelines for privacy notices and terms and conditions, that would be customizable to the specific needs of the postal sector.

Practical Implementation: While according to the practical implementation from recommendation 7, a guidelines for privacy notice are suggested to be developed, here more guidelines including for terms and conditions, e-mail information and consent forms are recommended to be developed, thus leveraging the UPU's role as a global standard-setter in the postal sector and its capacity to facilitate cooperation among member countries.

Recommendation A10

To enhance the universal understanding of data protection practices among all member countries, the UPU should offer training and resources to DOs, particularly in the developing regions, through workshops and webinars regarding the various data protection requirements.

Practical Implementation: A comprehensive training curriculum, especially also covering the fundamental principles of data protection, should be established to guarantee overall basic knowledge. It is recommended to follow the practical implementation of training under recommendation 3, 14 and 29.

The UPU can ensure that developing regions are making use of the training curriculum by actively engaging with DOs in these areas to tailor training to their specific needs and challenges. Additionally, the UPU could establish a monitoring and support system to regularly provide support where needed.

Recommendation A11

A monitoring mechanism should be in place to ensure that all member countries are adhering to their information and data protection obligations and are updating their information instruments regularly. This could involve regular surveys, audits, or peer reviews.

Practical Implementation: The UPU could establish a standardized reporting system where member countries submit periodic updates on their compliance with information obligations and updates of adjustments, they made to their information instruments. Additionally, the UPU might consider creating a peer review mechanism to ensure transparency and accountability among member countries.

Recommendation A12

All member countries should be encouraged to regularly review and update their privacy policies and consent forms. This should be done not only in response to changes in data processing activities but also to reflect changes in the legal and regulatory landscape.

Practical Implementation: The establishment of a set of guidelines by the UPU for privacy policy updates, including a recommended review cycle, can help ensure the privacy and security of data handled by the DOs. Additionally, the UPU should continuously maintain and update the centralized database.

Recommendation A13

To ensure compliance with Art. 10(1) of the UPU Convention, which outlines the purpose limitation for data processing, it is crucial to develop and implement systematic processes to ensure data is used only for its intended purposes.

Practical Implementation: To achieve this, the UPU should consider providing guidance on how to reach best practice. This can be done by fostering an active exchange among the member countries to share knowledge and experiences or by providing structured documents, including the creation of internal policies, conducting regular training, and establishing oversight mechanisms.

The UPU could encourage a standardized framework that mandates member countries to conduct regular audits and certify their compliance with purpose limitation principles. Additionally, the UPU might call for the integration of technical safeguards, such as access controls and data usage monitoring systems, to clarify adherence to Art. 10(1) of the UPU Convention across its member countries.

Recommendation A14

Implement and foster continuous data protection training programs specially focusing on improving the confidentiality and security of data exchanges.

Practical Implementation: The practical implementation as stated under recommendation 3 can be followed to pursue this recommendation, with a specific emphasis on confidentiality and security through modules.

Recommendation A15

All member countries should be encouraged to develop comprehensive written policies and procedures pertaining to roles and responsibilities. These documents should be regularly reviewed and updated to reflect current best practices and legal requirements.

Practical Implementation: The UPU could establish a standardized framework and provide guidelines for policy development to its member countries, ensuring consistency and compliance with international best practices. Additionally, the UPU could promote periodic reviews and updates of these policies as a condition of continued membership, with the provision of technical assistance and peer review mechanisms to facilitate compliance and continuous improvement.

Recommendation A16

Continual investment in and updating of technical measures are crucial as threats evolve. For those not using these measures, action is recommended to implement robust technical defenses.

Practical Implementation: The UPU could establish a dedicated cybersecurity task force responsible for developing a set of standardized technical defense protocols. This task force would also be assigned to create a phased implementation roadmap tailored to the varying capabilities of member countries. To promote universal compliance, the UPU could introduce a certification process, verifying the implementation of the prescribed technical defenses.

Recommendation A17

All member countries must have a data protection strategy.

Practical Implementation: By providing a standardized digital toolkit that provides member countries with the necessary information and protocols to establish robust data protection strategies, the development of such data protection strategies can be accelerated.

Additionally, the UPU could promote a global peer-review program where member countries periodically evaluate their data protection systems, ensuring compliance and facilitating the sharing of best practices for service continuity and rapid recovery in the event of disruptions.

Recommendation A18

Immediate action is required to address and understand the gaps in emergency plans and backup systems to ensure adherence to the MDSA and preparedness against potential outages.

Practical Implementation: The initiation by the UPU of an audit program that assesses the current state of emergency preparedness across MDSA signatory countries can as a first step help identify where exactly the gaps are. Following this, the UPU could establish a set of minimum emergency preparedness standards and periodically follow up on these with the signatory countries to improve adherence. This would create an enhancement of resilience against potential outages and ensure a higher MDSA adherence.

Recommendation A19

All countries responding that they do not monitor or report security incidents, especially for those subject to the MDSA, should take immediate action to establish a monitoring and reporting mechanism for security breaches relating to personal data.

Practical Implementation: It is highly recommended to create clear guidelines and channels for reporting incidents internally, and where necessary, to other stakeholders. A comprehensive policy should outline the procedures for monitoring and reporting security incidents.

Recommendation A20

All member countries should adopt a policy to outline who needs to be notified in case of security incidents and data breaches.

Practical Implementation: The UPU can support and accelerate this by providing supplementary documents containing best and the MDSA compliant practices and processes. The UPU could create a designated team for data protection matters. This team could especially also be contacted for guidance in the instances when data security breaches happen. By that, the UPU could support on the go and clarify the expectations that come along with such notification obligations.

Recommendation A21

It is recommended to enhance clarity regarding the definition of security incidents or data breaches to potentially improve response times.

Practical Implementation: Clear definitions are fundamental to any data protection framework and ensure that all member countries have a common understanding of the data protection practices. By establishing precise criteria for what constitutes a security incident or data breach, response protocols can be tailored and can lead to more efficient and effective time management of such events.
The UPU can clarify the terms and the common understanding in the MDSA. This should be based on international standards and best practices, while also allowing for local legal requirements and cultural considerations.

Recommendation A22

As a best practice, establish a plan and timeframe for regular security assessments as part of an overarching security assessment policy.

Practical Implementation: The assessments help identify vulnerabilities and maintain robust security over time. To establish a sound plan, it is recommended to further outline the requirements outlined in the MDSA. The effectiveness of security audits can be significantly hampered by poor cooperation among stakeholders. This is highlighted by the feedback received outlining a request for a better collaboration with PTC. To address this issue, it is imperative to foster communication and cooperation between all parties involved. This may involve the establishment of more explicit communication channels and clearly defined responsibilities.

The first step in implementing this recommendation is to develop a comprehensive security assessment policy that outlines the scope, frequency, and methodology of the assessments. This should be tailored to the specific needs and risks of the postal sector and should consider the varying capabilities and resources of member countries.

Member countries should create a detailed schedule that specifies when each assessment will take place. This could be annually, biannually, or at a different interval based on the risk environment and the resources available. Alongside the schedule, a checklist of assessment tasks should be developed to ensure consistency and thoroughness.

The results of the assessments, along with any actions taken, should be documented, and reported to relevant stakeholders. This ensures transparency and accountability.

Recommendation A23

It is critical to establish high-level clear retention schedules that do not supersede national and international requirements but outline best practices for those who do not have the necessary guidance from national legislation.

Practical Implementation: It is essential to develop comprehensive data retention policies that define the lifespan of different categories of personal data. These policies should keep in mind operational needs and best practices in data protection, as well as the purposes and necessity of data retention. These policies should be specific, justified, and documented. To offer support when developing this documentation, the UPU could provide opportunities for discourse and collaboration among member countries as well as supplementary documents offering guidance. This can promote a more harmonized yet still country specific approach to data protection in each country.

Recommendation A24

Clear guidelines and policies should be created on the proper disposal and deletion of no longer needed personal data to comply with the principles of data minimization.

Practical Implementation: The first step in implementing this recommendation is to develop comprehensive and clear data retention policies as outlined in recommendation 23. Then, it is recommended to implement and outline secure data disposal methods appropriate for the data and storage medium. For digital data, this could involve suing software tools that overwrite data before deletion. From an operational procedure perspective, it is recommended that automated systems flag data due for disposal and either automatically delete it or notify responsible personnel to carry out the process. For physical records, this could involve shredding or incineration. The policy should consider maintaining clear records of data disposal activities, including what data was disposed of, when, and by whom (i.e., deletion protocol). This documentation is crucial for accountability. Establishing such processes on data retention periods is a fundamental aspect of data protection and privacy practices that align with the principles of data minimization.

Recommendation A25

In developing regions, it is important to foster a minimal level of data subject rights which can be attained.

Practical Implementation: This recommendation requires a tailored approach that considers the unique challenges these regions face, which can include limited resources, infrastructure, and expertise in data protection. However, with international cooperation and a phased approach to implementation, it is possible to establish a baseline for data protection. To implement this recommendation, a focus on capacity building is essential. This can be done through partnerships with other member countries who can provide insights into their data protection practices. By providing robust policies like an improved MDSA, and raising awareness, the UPU can ensure that the data protection frameworks are understood and followed.

Recommendation A26

The UPU should promote the establishment of formal policies. This should include clear guidelines on how to respond to different types of requests, who is responsible for responding, what to document, and within what timeframe.

Practical Implementation: Formal policies are a cornerstone of effective data protection practices and can significantly enhance the consistency and reliability of responses to various requests. The guidelines should clearly delineate the roles and responsibilities in responding to the various types of data requests received from Parties or data subjects. Therein, outlining the timeframes should be realistic and in line with the MDSA requirements. The policy should outline a guidelines on what to document when receiving such requests, the actions taken, and the timeframe within which the response was provided.

Recommendation A27

It is recommended that the UPU support its member countries by providing comprehensive guidelines on the RoPA. These guidelines should outline the obligatory pieces of information required for completion and include examples for ease of understanding. By doing so, the UPU can ensure a certain level of standardization across postal services and promote the harmonization of data protection practices in the postal sector. Additionally, it is suggested that internal guidelines be established for the frequency of reviewing and updating the RoPA, with an annual review being the commonly accepted minimum.

Practical Implementation: The first step is to draft internal guidelines that define the scope, responsibilities, and procedures for the RoPA and its review. This should include identifying the team or individual responsible for drafting and reviewing the ROPA, the specific elements of the RoPA that are mandatory and thus need to be checked, and the process for making updates. Once this is defined, a schedule should be implemented that triggers the review process annually. This can be facilitated by using calendar reminders or other software tools. Furthermore, training shall be provided to ensure that all understand the importance of the RoPA and its review, and the steps involved in the process. By institutionalizing these practices, member countries can ensure that the RoPA is consistently up to date, as required by the MDSA and several national legislations, thereby supporting the overall data protection strategy.

Recommendation A28

The availability of regular training can be promoted by the UPU to accelerate and ease access to data protection best practices.

Practical Implementation: To increase attendance at these trainings, strategies such as targeted outreach, incentivization, and emphasizing the importance of a common understanding of data protection can be employed. Regarding training, it is recommended to follow the recommendations outlined in recommendation 3.

Recommendation A29

The PTC could analyze optimization possibilities concerning the technical environment among the member countries to reduce technical delays and fragmentations. Additionally, considering the importance of maintaining a secure postal network, it is recommended that the PTC expands its role to include conducting IT audits at the designated operators (DOs). By conducting these audits, the PTC could identify vulnerabilities, strengthen security measures, and ensure a robust defense against potential threats, ultimately enhancing the overall integrity and reliability of the postal network.

Practical Implementation: The PTC could initiate a comprehensive examination of the existing technical infrastructure across member countries, employing a team of experts to identify bottlenecks and areas for technological harmonization. Following this, the PTC could develop a standardized set of protocols and technologies that can be adopted by the member countries, thus facilitating smoother cross-border train operations, and reducing technical delays.

5.2.2. Recommendations to amend the UPU policy and regulatory framework

Recommendation B1

Maintain the Convention provisions on processing of personal data, as they serve as cornerstones of current data protection laws and regulations. If the Convention is under review, it is recommended to consider broadening the existing provisions to encompass not only national obligations but also international obligations (like the PPSA). This would ensure that designated operators adhere to both domestic and international standards for data protection, fostering a comprehensive and globally harmonized approach to safeguarding personal data within the postal sector.

Practical Implementation: When the Convention is revised, a dedicated working group should be established to review and expand the existing Convention provisions regarding the processing of personal data. This group should be composed of legal experts, representatives from member countries, and other relevant stakeholders. Their mandate should include analysis of international data protection standards alongside postal-specific regulatory frameworks, such as the Postal Payment Services Agreement (PPSA), they should propose specific amendments to align the Convention with these standards and frameworks. This approach should foster a more robust, comprehensive, and harmonized strategy for safeguarding personal data within the postal sector.

Recommendation B2

Maintain the PPSA provisions for data protection as they closely align with international best practices.

Practical Implementation: The provisions for data protection within the PPSA should be preserved, given their alignment with international best practices. To ensure continued relevance and compliance with emerging standards and data protection laws, periodic reviews should be conducted. These reviews should involve updates based on the latest developments in global data protection regulations and best practices, ensuring the PPSA remains a model of robust and up to date data protection within the postal sector.

Recommendation B3

To enhance clarity and consistency in the interpretation and application of the MDSA, it is recommended to expand and strengthen definitions to include a broader range of data protection and privacy concepts by incorporating common definitions from other relevant texts, including but not limited to the OECD Guidelines, the GDPR and the SADC Model Law.

Practical Implementation: Form a specialized working group tasked with reviewing and incorporating key terms and definitions from other relevant texts, including but not limited to the OECD Guidelines, the GDPR and the SADC Model Law. This group should focus on integrating definitions for critical terms like "processing", "consent" and "personal data breach" into the MDSA. The objective is to ensure these definitions are consistently understood and applied regardless of member countries jurisdiction.

Recommendation B4

It is recommended to provide explicit definitions of the "controller", "processor" and "sub-processor" roles within the MDSA taking into consideration commonly recognized definitions contained in other relevant texts, including but not limited to in the OECD Guidelines, the GDPR and the SADC Model Law.

Practical Implementation: Explicit definitions of the "controller," "processor," and "sub-processor" roles should be incorporated within the MDSA, taking into consideration the context of the MDSA's operational framework to ensure that they are both applicable and practical for the parties involved. These definitions should also take

into account commonly recognized definitions contained in other relevant texts, including but not limited to the OECD Guidelines, the GDPR and SADC Model Law.

Recommendation B5

Enhance the existing data protection principles included in the MDSA and incorporate additional fundamental data protection and privacy principles, such as data minimization, purpose limitation, transparency, data security, and retention. These principles should reflect the relevant universal standard, allowing countries to agree upon them regardless of their legal framework.

Practical Implementation: Enhance the existing data protection principles in the MDSA by explicitly incorporating additional fundamental data protection and privacy principles such as data minimization (i.e. only personal data that is needed for the envisaged purpose should be collected), purpose limitation (i.e. personal data shall only be collected for specific and explicitly communicated purposes and not be processed for other purposes), transparency (i.e. conducted processing shall be transparent for the data subjects), data security (i.e. security and confidentiality of personal data must be guaranteed while processing), and retention (i.e. personal data shall be retained no longer than is necessary for the purposes for which the personal was collected for initially). Additionally, a framework for updating these principles should be developed to ensure they remain aligned with evolving international privacy frameworks and standards.

Recommendation B6

Introduce basic data protection measures focused on outcomes. Instead of providing a list of specific technical solutions that might be difficult to implement, MDSA should recommend general outcomes, such as “ensuring data is sufficiently protected against unauthorized access” and similar provide specific examples (like encryption, anonymization, etc.) without mandating them. Additionally, incorporate, to the extent possible, the basic requirements relating to protection of personal data by design and default.

Practical Implementation: Within the MDSA, develop a framework that focuses on outcome-based data protection measures, allowing flexibility in how these outcomes are achieved. This framework should outline key objectives along with examples of specific measures that might be adopted, for example:

- Ensuring data is sufficiently protected against unauthorized access (for example, implement access controls and authentication mechanisms, such as user authentication and role-based access controls)
- Implementing measures to prevent data breaches and unauthorized disclosures (for example, encrypting personal data during transmission and storage to protect against unauthorized access)
- Establishing procedures for secure data storage and transmission (for example. implement encryption and pseudonymization techniques to protect personal data during storage and transmission)

Recommendation B7

Provide requirements within the MDSA regarding the scope and level of detail for a RoPA.

Practical Implementation: Specify the required elements of a RoPA within the MDSA. This may include:

- Details of the data controller and data processor(s) involved in the processing activities.
- Purposes of the processing, including the legal basis for processing.
- Categories of personal data being processed.
- Recipients or categories of recipients to whom the personal data may be disclosed.
- Transfers of personal data to third countries or international organizations, if applicable.
- Retention periods for the personal data.
- Description of technical and organizational security measures implemented to protect the personal data.
- Records of any data breaches or security incidents related to the processing activities.
-

Recommendation B8

Relevant principles regarding security incidents and data breaches may be incorporated in the MDSA to ensure a uniform understanding among member countries on such aspects. Such principles may also include basic data breach notification requirements.

Practical Implementation: Clearly define what constitutes a security incident and a data breach within the MDSA. These definitions should be designed to ensure a consistent understanding among member countries. Additionally, the UPU should introduce basic data breach notification requirements as part of the MDSA. This will establish a framework for timely and effective response to incidents, promoting transparency and accountability in data protection practices within the postal sector.

Recommendation B9

Set clearer guidelines on data retention periods, suggesting a review of the necessity of holding personal data periodically, with the possibility of shortening the maximum retention period from 10 years to a more reasonable timeframe where appropriate. Additionally, define deletion process to be followed after the retention period has elapsed.

Practical Implementation: Provide more specific guidelines on data retention periods. This will ensure clarity and consistency in data retention practices. Additionally, provisions should be included in the MDSA to define processes for data disposal after the retention period has elapsed. This will address potential inconsistencies and uncertainties regarding data retention and disposal.

Recommendation B10

To ensure awareness and execution of data protection principles, it is advisable to amend the MDSA with a view to including a strong recommendation for signatories to appoint a person or a team responsible for ensuring data protection compliance.

Practical Implementation: Integrate a strong recommendation into the MDSA relating to the appointment of a dedicated person or a team who would be tasked with overseeing the implementation of data protection measures and ensuring compliance with the MDSA, acting as the primary point of contact for data protection issues, both internally and externally, reporting on data protection compliance, facilitating transparency and accountability, etc. By designating a responsible individual or a team, the Parties can establish clear accountability and promote effective implementation of data protection measures outlined in the MDSA.

Recommendation B11

To enhance oversight and strengthen accountability, it is recommended to include provisions that emphasize the importance of documentation and regular assessments to ensure compliance with privacy practices. This should involve mandating parties to maintain records that demonstrate adherence to privacy practices, including implemented data protection measures and relevant policies or procedures. Additionally, it is advisable to establish a requirement for regular assessments, such as surveys and questionnaires, to evaluate the effectiveness of privacy practices and identify areas for improvement.

Practical Implementation: The UPU should include provisions in the MDSA that require parties to maintain records demonstrating adherence to privacy practices and implemented data protection measures. Additionally, establish a requirement for regular assessments, such as surveys and questionnaires, to evaluate privacy practice effectiveness and identify areas for improvement. This will enhance oversight, strengthen accountability, and promote continuous improvement in data protection within the postal sector.

Recommendation B12

To enhance cooperation, it is recommended to include provisions in the MDSA that require parties to actively support and assist one another in fulfilling their obligations contained in the Acts of the Union and the MDSA regarding data protection. This will foster a stronger collaborative environment and ensure a more effective implementation of data protection measures across.

Practical Implementation: Incorporate a collaborative framework within the MDSA that mandates mutual support among member countries for fulfilling data protection obligations..

Recommendation B13

The flexibility of the MDSA should be maintained and continued with a robust baseline for data protection that all members can adhere to. The MDSA already allows for customization to accommodate regional or national requirements within the standardized framework of the MDSA, recognizing that different regions or countries may have unique data exchange needs and provide flexibility for adaptations that align with the core principles of the MDSA without compromising its overall effectiveness. It is recommended that the relevant bodies of the UPU explore whether the possibilities (and flexibility) under the current MDSA may be further enhanced.

Practical Implementation: The UPU should maintain the flexibility of the MDSA while establishing a robust baseline for data protection that all members can adhere to. This can be achieved by allowing customization

within the standardized framework of the MDSA to accommodate regional or national requirements as well as conditional obligations. Yet it may also be noted that the MDSA itself already provides for the possibility of adoption of regional-specific annexes aimed at addressing more stringent parameters as applicable to certain geographical regions or groups of UPU member countries. It may thus be explored whether such possibility may be further enhanced

6. Conclusions

Overall, the UPU provides a basic framework for data protection within the postal sector through the Convention and its Regulations. Nevertheless, the report has identified several best practices and gaps therewith that require further development.

The results indicate that there are varying degrees of implementation of the Convention and the MDSA among member countries and signatories, hence, leading to lack of coordination and harmonization and potential challenges for cross-border cooperation and efficiency.

Based on the desk research, interviews with key stakeholders and the survey results, the report defines several recommendations for the UPU to facilitate a common baseline practice towards data protection. This includes offering training and guidelines, establishing monitoring mechanisms, providing clear guidance on roles and responsibility and policies.

Engaging in a formal dialogue with relevant domestic and/or regional authorities (including without limitation the EU) could be seen as beneficial for achieving better identification and, as appropriate, harmonization of the practices in place. This dialogue could involve the development of standard clauses and processes for international data transfers. In the context of international postal service, personal data should be minimized to what is necessary, with a focus on mitigating the risk of harm to data subjects. Yet, challenges may arise when submitting standard contractual clauses for review, as not all versions satisfy such domestic and/or regional requirements. Additional challenges include mis-delivery being classified as a data breach and the risk of cyber-attacks. Clear frameworks and collaboration are necessary to address these issues effectively. Naturally, the report acknowledges that the implementation of the recommendations may vary depending on the context and resources of each member country. However, it also emphasizes that the UPU plays a key role in providing clear and consistent definitions for data protection processes in the postal sector and facilitating training and collaboration among its members. These are essential elements for ensuring harmonization of data protection practices across the UPU member countries.

The report suggests that the UPU can review and update its existing agreements and guidelines, such as the Convention and MDSA, to enhance their clarity and practicality, and to monitor and evaluate their implementation and effectiveness.

References

Convention for the Protection of Individuals with regard to Automated Processing of Personal Data (Convention 108)

General Data Protection Regulation (GDPR, Regulation 2016/679 of the European Parliament)

Lei Geral de Proteção de Dados Pessoais (LGPD, Lei n° 13.709/2018)

Multilateral Data Sharing Agreement (MDSA)

Postal Payment Services Agreement (PPSA)

Revised Kyoto Convention

Universal Postal Convention

UPU Guidelines on Data Capture and Compliance with CN 22/23

UPU Guidelines on Exchange of Electronic Advance Data between Designated Operators and Customs Administrations

World Customs Organization – UPU Postal Customs Guide