



PAKISTAN

Digital Trade Acceleration Initiative

Country Report



Disclaimer

The following legal disclaimer (“Disclaimer”) applies to this document (“Document”) and by accessing or using the Document, you (“User” or “Reader”) acknowledge and agree to be bound by this Disclaimer. If you do not agree to this Disclaimer, please refrain from using the Document.

This Document is prepared by the Digital Cooperation Organization (DCO). While reasonable efforts have been made to ensure accuracy and relevance of the information provided, DCO makes no representation or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability of the information contained in this Document.

This Document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Additionally, every effort was made to collect comprehensive data for this Document, which was shared with each of the DCO Member States and, through them, with relevant government agencies. The data collected was current as of September 2024, and there may have been developments or updates since that time. DCO does not undertake any responsibility for such subsequent developments or the use of data that may no longer be current.

The information provided in this Document is intended for general informational purposes only and should not be considered as professional advice. DCO disclaims any liability for any actions taken or not taken based on the information provided in this Document.

DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between DCO and the User.

The use of this Document is solely at the User’s own risk. Under no circumstances shall DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the Digital Cooperation Organization. The User shall not reproduce any content of this Document without obtaining DCO’s consent or shall provide a reference to DCO’s information in all cases. By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon posting.

© Digital Cooperation Organization 2025.
All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

How to Read This Report

This comprehensive report is structured to guide readers to the information that interests them most. Three sections illuminate the regulatory assessment from different perspectives:

Section A is the core of this report. It assesses the domestic regulatory environment across twelve policy areas, with three subsections for each.

1. Our guiding questions analyse how each policy area interacts with digital trade.
2. Our summaries condense the regulatory environment through brief descriptions of the main legal frameworks and oversight authorities.
3. Our source lists provide a repository of official sources to facilitate further analysis.

Section B provides a factsheet that describes the local digital economy across four key dimensions: size and activities, digital infrastructure and connectivity, digital skills, and digital government.

Section C outlines international commitments and references the international fora in which it engages on digital issues.

Table of Contents

01	Domestic Regulatory Environment Assessment	6
	Data Protection	8
	Cross-Border Data Transfers	11
	Location of Computing Facilities	14
	Online Consumer Protection	16
	Electronic Transactions	19
	Trade Facilitation with Digital Means	22
	Cybersecurity	25
	Artificial Intelligence	28
	Source Code	31
	Digital Economy Taxation and Customs Duties	34
	Electronic Payments	37
	SMEs and Digital Inclusion	40
02	Digital Economy Factsheet	43
	Size and Activities of the Digital Economy	45
	Digital Infrastructure and Connectivity	46
	Digital Skills	47
	Digital Government	48
03	International Commitments and Collaboration	49
	Commitments	51
	Fora	53

Executive Summary

The purpose of this report is to provide a detailed description of the regulatory environment affecting businesses and consumers engaging in digital trade. We illuminate the regulatory environment from three perspectives:

- 01 A comprehensive regulatory assessment explains the regulatory environment across twelve policy areas.
- 02 A factsheet describes the local digital economy across four dimensions: size and activities, digital infrastructure and connectivity, digital skills, and digital government.
- 03 An overview of existing international commitments characterises efforts to accelerate digital trade.

The regulatory assessment is the main contribution of this report and provides the following findings:

Data Protection:

User consent is not generally required for data processing. Users have the right to access information and can request correction and deletion of credit information. Registration and local representation are required for “significant social media companies”, not all data processors.

Cross-Border Data Transfers:

Pakistan does not currently establish distinct rules for cross-border data transfers. Pakistan is deliberating the Personal Data Protection Bill 2023, which would

comprehensively govern cross-border data transfers.

Location of computing facilities:

Pakistan does not mandate data localisation in general but has several sectoral data localisation mandates, including for critical telecommunications data, telecommunications data related to consumer interactions and transactions, data from public wi-fi, mobile banking data, and financial transactions data.

Online Consumer Protection:

Pakistan protects online consumers under the general consumer protection framework, consisting of subnational and sectoral rules that prohibit unfair practices. E-commerce platforms must obtain licences to operate, establish consumer complaint mechanisms. The sending of unsolicited messages (spam) is prohibited without recipients' express permission.

Electronic Transactions:

Electronic transactions are recognised as equivalent to paper-based transactions, with exceptions. The framework distinguishes between standard and advanced electronic signatures. The government provides an online ID for government services (Pak-Identity).

Trade Facilitation with Digital Means:

Pakistan provides electronic trade administration documents and accepts submissions in electronic form. The national single window is operational and facilitates the fulfilment of import, export, and transit-related requirements.

Cybersecurity:

Cybersecurity obligations are based on risk level, for example for critical infrastructure. Entities affected by cybersecurity incidents must notify authorities.

Artificial Intelligence:

There is currently no binding regulatory framework on the governance of AI. The government is developing the National AI Policy 2024, which aims to establish a legal framework for AI.

Source Code:

The copyright framework protects computer programmes as “literary works”, establishing protections, with certain exceptions, and prohibiting sharing without authorisation. Pakistan does not require source code sharing.

Digital Economy Taxation and Customs Duties:

Digital services and digital products are not subject to customs duties but are subject to the sales tax. E-commerce imports are subject to both customs duties and sales tax. Pakistan further levies a direct tax on providers of digital services/digital products.

Electronic Payments:

Know-your-customer, anti-money-laundering, and counter-terroism-financing rules apply to digital payments. Payment providers, including e-commerce gateways, must obtain a licence from the central bank.

SMEs and Digital Inclusion:

Pakistan has implemented several policy initiatives and programmes to support SMEs and disadvantaged groups in leveraging digital trade opportunities. These measures include the development of a national e-commerce policy, strategic frameworks targeting SME participation in digital marketplaces, and collaborative efforts between government agencies to enhance SME capacity for digital exports. vPakistan has implemented several policy initiatives and programmes to support SMEs and disadvantaged groups in leveraging digital trade opportunities. These measures include the development of a national e-commerce policy, strategic frameworks targeting SME participation in digital marketplaces, and collaborative efforts between government agencies to enhance SME capacity for digital exports.



01

Domestic Regulatory Environment Assessment

Domestic Regulatory Environment Assessment

For thriving digital trade among the members of the Digital Cooperation Organization, their regulatory environment should be comprehensive and adaptive. Absence of fundamental regulatory building blocs, regulatory divergence, or explicit barriers can hinder the DCO MS's digital trade reaching its potential.

This section assesses the regulatory environment across twelve policy areas on three layers. First, we answer guiding questions to analyse each policy area's impact on digital trade. Second, we summarise the regulatory environment through brief descriptions of the main legal frameworks and oversight authorities. Third, we provide a repository of official sources to facilitate further analysis.

We conduct this assessment for the following policy areas:

- 01 Data Protection
- 02 Cross-Border Data Transfers
- 03 Location of Computing Facilities
- 04 Online Consumer Protection
- 05 Electronic Transactions
- 06 Trade Facilitation with Digital Means
- 07 Cybersecurity
- 08 Artificial Intelligence
- 09 Source Code
- 10 Digital Economy Taxation and Customs Duties
- 11 Electronic Payments
- 12 SMEs and Digital Inclusion



Data Protection

The purpose of this section is to comprehensively characterise the conditions for domestic data collection and processing. Alignment with international best practices in data protection is important for fostering trust whilst facilitating market access. Deviation from these practices could potentially impact digital trade. If the data protection requirements within the member state are too low, that diminishes trust. If data protection requirements are too high, that may delay market entry from international service providers.

Guiding Questions

We analyse whether user consent is required for the processing of personal data. We then delineate the rights of data subjects and obligations for those processing data, specifically on local representation and registration. Finally, we identify the authority responsible for overseeing and enforcing data protection regulations.

In Pakistan, user consent is not generally required for data processing, although the breach of confidentiality of information without consent is prohibited. Users are generally granted the right to access their information and, for credit information, can request correction and deletion. Registration and local representation are required for “significant social media companies”, but not for all data processors. Oversight is divided between the Ministry of Information Technology and Communication, the Telecommunication Authority, and the Information Commission. The Telecommunication Authority received 180,602 consumer complaints in 2022-2023 (not all related to data protection), resolving 98.6% thereof.

Summary

○ Pakistan has no active data protection law. Its current framework consists of legislation such as the Prevention of Crimes Act (PECA) and the Electronic Transactions Ordinance, whose focus on data protection is limited. Subsequent to this is the Right of Access to Information Act, which works to ensure transparency and accountability in how public authorities handle personal information. The Act also applies to public-private partnerships and any non-public organisation that undertakes a public function. It amplifies citizens' right to access and review records. The Right of Access to Information Rules outline procedures for handling information requests.

○ In a recent initiative, the Personal Data Protection Bill was introduced in May 2023, gaining approval from the Federal Cabinet, and is subsequently awaiting presentation before the National Assembly. The Bill aims to give citizens more control over their personal data, decreeing that organisations should obtain explicit consent from individuals before handling their data. It outlines various data subject rights pertaining to data collection and processing, and emphasises transparency and accountability for data controllers and processors. To this end, the Bill would require all data controllers and processors to register with the Commission if they fall under Pakistan's jurisdiction and demand that "significant" data controllers and processors appoint a data protection officer.

○ The oversight authorities responsible for data protection are:

The National Commission for Personal Data Protection, which is responsible for managing personal data protection matters.

The Ministry of Information Technology and Communication, which spearheads initiatives such as the development of the Personal Data Protection Bill amongst other legislation. It ensures compliance with laws, advises on best practices for data privacy and collaborates with other government bodies to enhance protection measures.

The Pakistan Information Commission, which executes data protection standards by enabling mechanisms that allow citizens to exercise their constitutional right of access to information in matters of public importance. One of their key functions is to decide complaints and take action against those who fail to comply with the provisions of the Right of Access to Information Act 2017.

Finally, the Removal and Blocking of Unlawful Online Content Rules require online platforms to remove or block unlawful data, including personal and sensitive personal data, to prevent misuse. Authorities must maintain records of these actions to ensure accountability and transparency. "Significant" social media companies must register with authorities and appoint local representatives.



SOURCES

Primary Legislation

- Electronic Transactions Ordinance 2002
- Draft of the Personal Data Protection Bill 2023 [source not working]
- Prevention of Electronic Crimes Act 2016
- Right of Access to Information Act 2017
- Balochistan Right to Information Act (Act No. II of 2021)
- The Sindh Transparency and Right to Information Act 2016 [source not working]
- The Khyber Pakhtunkhwa Right to Information Act 2013
- Punjab Transparency and Right to Information Act 2013.

Secondary Legislation

- Ministry of Information Technology and Telecommunication: The Removal and Blocking of

Unlawful Online Content Rules 2020 [source not working]

- The Right of Access to Information Rules 2019
- Sindh Information Commission: The Right of Access to Information Rules, 2019 [source not working]

Oversight Authorities

- Ministry of Information Technology and Telecommunication [source not working]
- Pakistan Information Commission
- Balochistan Information Commission [no website available]
- Sindh Information Commission [source not working]
- Khyber Pakhtunkhwa Information Commission
- Punjab Information Commission [source not working]



Cross-Border Data Transfers

The purpose of this section is to analyse the conditions for the cross-border transfer of personal information. On the one hand, data flows are the bloodline of the digital economy. On the other hand, data flows are a controversial subject in geopolitical discussions, as governments worry that transferring data across borders may jeopardise its protection. How a government regulates data transfers reveals the balancing act between free data flows and protection of data abroad.

Guiding Questions

We differentiate whether the framework treats cross-border transfers differently from in-country transfers. We then analyse the specific conditions for cross-border transfers, ranging from data subject consent, to governmental adequacy decisions, to certification and contractual mechanisms. Finally, we delineate conditions for specific types of cross-border transfers and distil public policy objectives invoked by the government, where explicitly stated.

Pakistan does not currently establish distinct rules for cross-border data transfers. Pakistan is deliberating the Personal Data Protection Bill 2023, which would comprehensively govern cross-border data transfers. Specifically, it would require that personal data be transferred outside Pakistan only if the recipient provides adequate data protection measures.

Summary

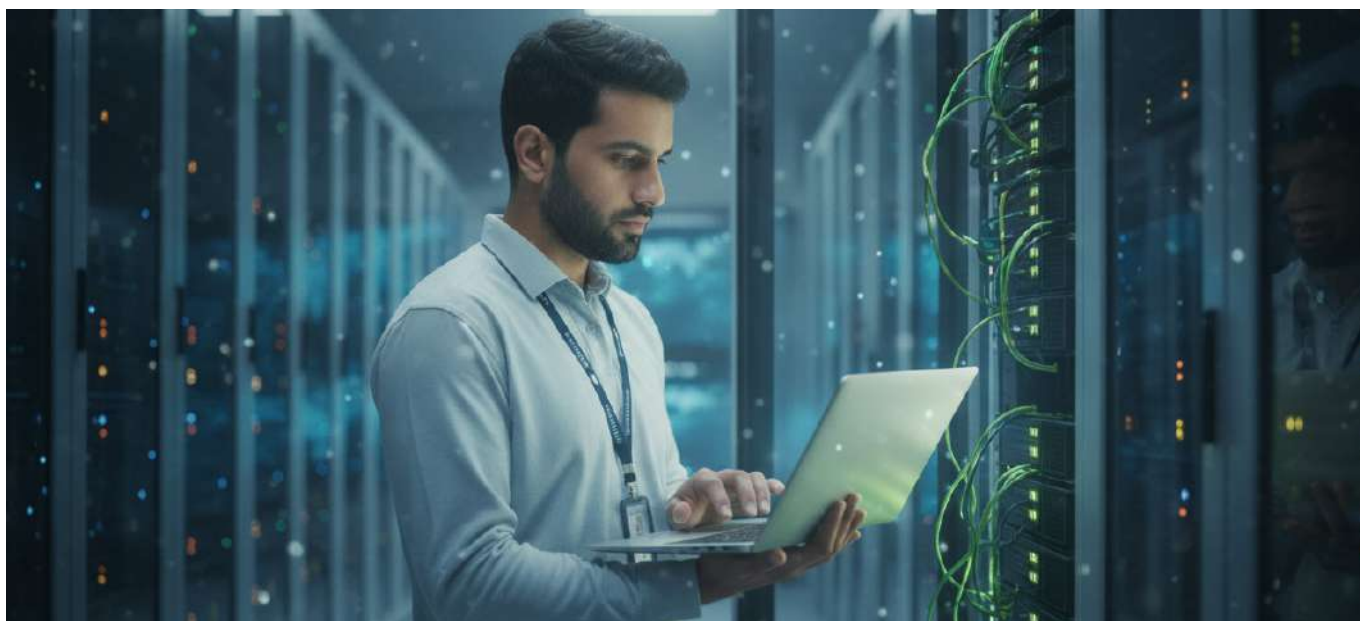
- Pakistan does not currently establish a specific regime for cross-border data transfers. The Personal Data Protection Bill, which is currently under deliberation, would allow personal data to be transferred only if the recipient provides adequate data protection measures. In addition, the Bill would mandate that critical data must always be processed and stored on servers within Pakistan, subject to approval from authorities (see section on Location of Computing Facilities).



SOURCES

Primary Legislation

- Personal Data Protection Bill Final Draft 2023



Location of Computing Facilities

The purpose of this section is to crystallise instances in which data must be stored in local computing facilities. Data localisation mandates require foreign providers to invest in or rent local infrastructure. This can create a significant barrier to digital trade due to burdensome procedural requirements or costs. Such requirements are thus subject to international scrutiny regarding their justification and scope.

Guiding Questions

We analyse whether the framework generally requires data to be stored in the national territory. We then analyse whether data localisation requirements apply to specific data types, such as infrastructure or health data. For each identified localisation requirement, we distil the public policy objective invoked by the government, if it is explicitly stated.

Pakistan does not mandate data localisation in general but has several sectoral data localisation mandates. Data that must be localised includes critical telecommunications data, telecommunications data related to consumer interactions and transactions, data from public wi-fi, mobile banking data, and financial transactions data. The objectives invoked include data sovereignty and data access by regulatory bodies. Currently, the government is deliberating the Personal Data Protection Bill, which would demand critical personal data to be localised.

Summary

- Pakistan does not generally mandate data localisation, but does establish sector-specific localisation requirements.
- The Pakistan Telecommunications Authority (PTA) has issued several policies requiring data localisation, including:



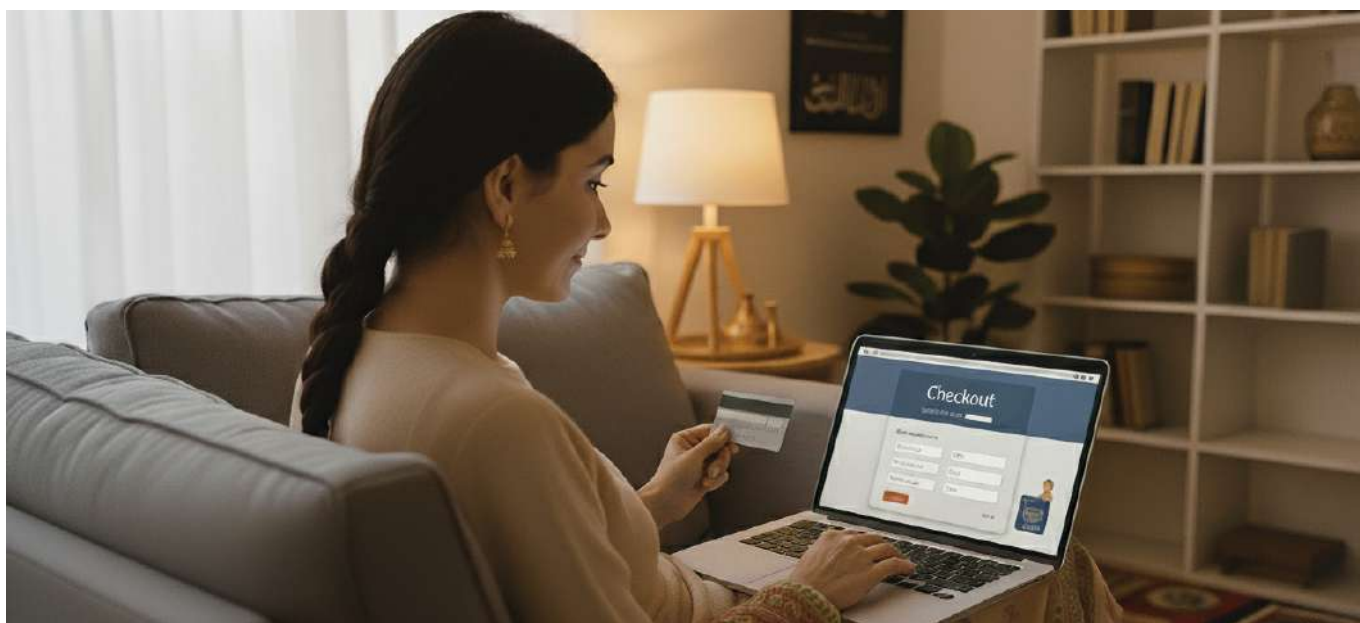
SOURCES

Primary Legislation

- Anti-Money Laundering Act 2010
- Payment Systems and Electronic Fund Transfers Act 2007

Secondary Legislation

- Pakistan Telecommunications Authority: The Critical Telecom Data and Infrastructure Security Regulation 2020
- Pakistan Telecommunications Authority: Data Retention of Internet extended to Public WiFi-Hotspots Regulations 2018
- Ministry of Information Technology and Telecommunications: Regulations for Technical Implementation of Mobile Banking 2016



Online Consumer Protection

This section provides a detailed overview of the approach to protecting online consumers. A well-regulated online consumer protection framework is crucial for fostering trust and confidence in online transactions. In the context of international trade, the implementation of strong online consumer protection regulations enables secure cross-border transactions and promotes the expansion of e-commerce.

Guiding Questions

We contour whether the online consumer protection framework is specific to online consumption or applies general rules thereto. We then delineate the practices that are considered violations of consumer protection and distil any special obligations for e-commerce platforms. We further analyse the regulatory approach regarding spam. Finally, we explain which authority oversees online consumer protection.

Pakistan does not have a dedicated regulatory framework for online consumer protection and instead applies its general consumer protection rules. At the national level, these rules are enshrined in various sectoral laws, rather than a centralised consumer protection law. The Payment Systems and Electronic Funds Transfers Act prohibits financial institutions from charging accounts without authorisation. Credit bureaus and telecommunications providers are further prohibited from making misrepresentations that mislead consumers. E-commerce platforms must

obtain licences to operate, establish consumer complaint mechanisms. Spam is criminalised and defined as the transmission of harmful, fraudulent, misleading, illegal, or unsolicited messages in bulk without recipients' express permission. Oversight is split between the central government and sectoral bodies, including the Telecommunications Authority. In 2022-2023, the Authority resolved 98.6% of the 180,602 consumer complaints it received (not all related to consumer protection).

Summary

- There is no comprehensive national consumer protection law in Pakistan. At the subnational level, the Islamabad Consumer Protection Act was one of the earliest comprehensive legal frameworks to govern consumer rights within Pakistan. At the sectoral level:

The Securities and Exchange Commission of Pakistan Act regulates consumer protection in capital markets.

The Payment Systems and Electronic Funds Transfers Act grants consumers the right to information regarding the goods or services they are purchasing, including digital transactions.

The Credit Bureaus Act regulates credit bureaus to ensure the safety of consumer credit information and penalises the spreading of false information, also covering entities such as utility providers and retailers.

The Pakistan Telecommunication (Re-organisation) Act regulates telecommunication services by

obligating licensees operating telecommunication systems in Pakistan, such as Internet Service Providers (ISPs) and mobile network operators, to meet minimum standards for the grade and quality of service requirements to protect consumers.

The Prevention of Electronic Crimes Act addresses spam and spoofing, and defines unsolicited information as unwanted commercial content sent against explicit rejection of the recipient.

The Pakistan Medical and Dental Council Ordinance encourages all health practitioners, public or private, to follow the code of medical ethics, including anti-discrimination practices for all patients.

- The Consumer Rights Commission of Pakistan is an independent body which investigates consumer complaints and advocates for the application of consumer-friendly policies. It collaborates with other authorities:

The Directorate General of Trade Organisations operating under the Ministry of Commerce regulates fair trade practices and imposes penalties for violations.

The Securities and Exchange Commission of Pakistan monitors capital markets, promotes investor protections and starts investigations, imposing fines where necessary.

The State Bank of Pakistan oversees the financial sector, addressing consumer complaints related to banking services and financial products.



SOURCES

Primary Legislation

- Islamabad Consumer Protection Act 1995
- The Securities and Exchange Commission of Pakistan (SECP) Act 1997
- Payment Systems and Electronic Funds Transfers Act 2007
- Credit Bureaus Act 2015
- Credit Bureaus (Amendment) Act 2016
- Pakistan Telecommunication (Re-organisation) Act 1996
- Pakistan Telecommunication (Re-organisation) (Amendment) Act 2006
- Prevention of Electronic Crimes Act 2016

Secondary Legislation

- Pakistan Telecommunication Authority: Protection from Spam, Unsolicited Fraudulent and Obnoxious Communication Regulations 2009

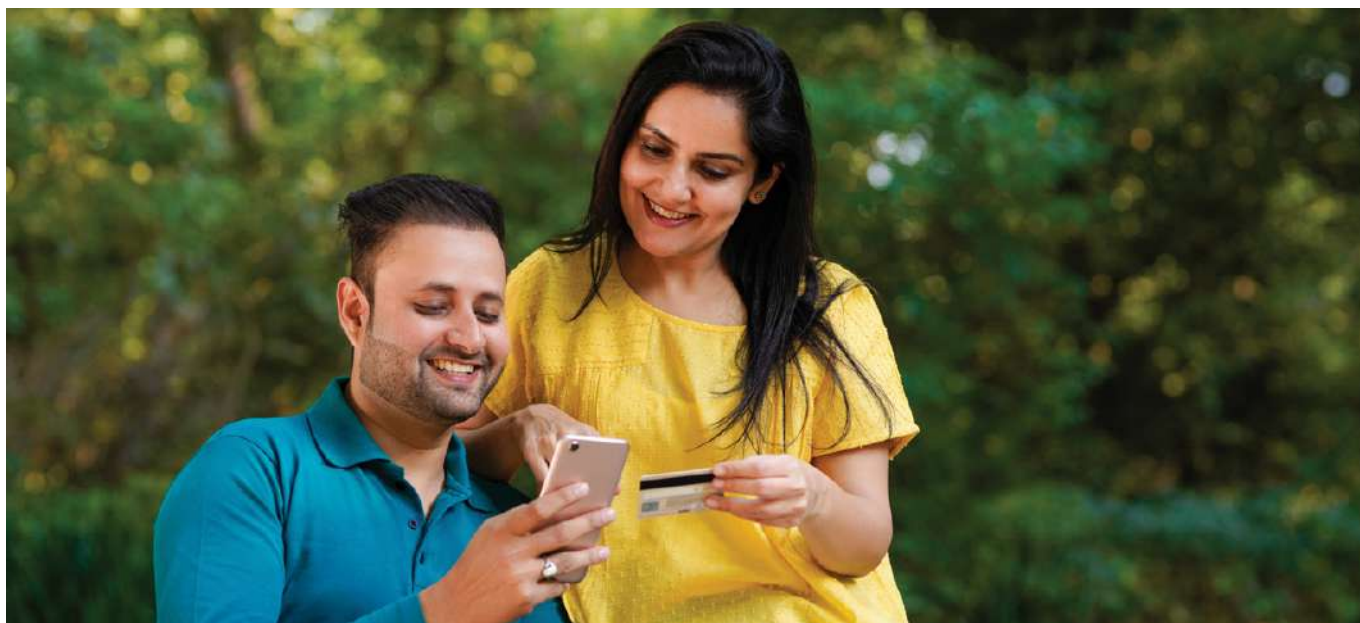
- Pakistan Telecommunication Authority: Telecom Consumers Protection Regulations 2009
- Pakistan Telecommunication Authority: Telecom Consumers Protection (Amendment) Regulations, 2016

Guidelines

- Ministry of Commerce: E-Commerce Policy of Pakistan 2019

Oversight Authorities

- Consumer Rights Commission of Pakistan (CRCP) [source not working]
- Ministry of Commerce/Directorate General of Trade Organisations (DGTO)
- Securities and Exchange Commission of Pakistan (SECP)
- State Bank of Pakistan
- Pakistan Telecommunication Authority (PTA)



Electronic Transactions

The purpose of this section is to identify whether there are any regulatory hurdles to electronic transactions compared to paper-based or face-to-face transactions of equivalent substance. A transaction contains different aspects such as the validity of the contract, signature, and authentication.

Guiding Questions

We focus on whether the electronic transactions framework is binding and whether it recognises electronic transactions as equivalent to paper-based transactions. We then differentiate the various types of electronic signatures in the framework. Finally, we distil whether electronic authentication is permitted and whether the government provides such authentication.

The electronic transactions framework is binding and spread across various legal acts, most importantly the Electronic Transactions Ordinance. The Ordinance establishes that electronic transactions are recognised as equivalent to paper-based transactions, with exceptions for documents such as wills and real estate transactions. The framework distinguishes between standard and advanced electronic signatures. The government provides an online ID for government services (Pak-Identity).

Summary

○ The Electronic Transactions Ordinance grants electronic signatures the same legal validity and enforceability as traditional paper-based signatures, ensuring their use is legally recognised across sectors. This ordinance empowers the Certification Council to oversee digital authentication and security measures. The framework differentiates between electronic signatures and advanced electronic signatures. Finally, the Prevention of Electronic Crimes Act (PECA) emphasises the need for secure practices in handling electronic signatures and documents and deems crimes, such as electronic forgery within electronic transactions, as punishable by law. The government provides an online identification system, Pak-Identity, to facilitate secure access to government services, inclusive of digital transactions.

○ The Pakistan IT Policy Action Plan, issued by the Ministry of Information Technology and Telecommunication (MoITT), aims to validate digital signatures and electronic authentication through legislative and regulatory proposals, such as the Digital Signature Act. It also offers incentives to IT firms who adopt digital payment systems. The Digital Pakistan Policy compounds this by outlining the efficiency of electronic transactions and facilitating seamless financial interactions with the introduction of online payments systems. Moreover, the E-Commerce Policy of Pakistan also addresses the legal landscape for electronic transactions by recognising the validity of digital contracts.

○ Several frameworks touch upon electronic transactions in the financial sector:

○ The Payment Systems and Electronic Fund Transfers Act requires secure authentication methods and gives the State Bank of Pakistan the power to designate payments systems and instruments to authenticate transactions electronically.

The Electronic Fund Transfers Regulations ensure that electronic transactions are only processed with explicit authorisation from the account holder of a bank account, and advocate for stringent verification processes.

The Regulations for Electronic Money Institutions establishes security measures and reporting requirements.

The Customers' Digital Onboarding Framework, revised in April 2022, emphasises the importance of valid identification documents and identity verification and screening tactics.

The Regulations for Mobile Banking Interoperability obligate authorised financial institutions and third-party service providers to ensure the data and transaction integrity.

The Regulations for Payment Card Security require card payment systems to implement robust authentication measures e.g., two or three factor authentications and ensure that consent is captured through secure digital signatures or verified contact channels.



SOURCES

Primary Legislation

- Electronic Transactions Ordinance 2002
- Payment Systems and Electronic Fund Transfers Act 2007
- Prevention of Electronic Crimes Act 2016
-

Secondary Legislation

- State Bank of Pakistan: Customers' Digital Onboarding Framework Revised on April 30 2022
- State Bank of Pakistan: Electronic Fund Transfers Regulations
- State Bank of Pakistan: Regulations for Electronic Money Institutions (EMIs) 2019
- State Bank of Pakistan: Regulations for Mobile Banking Inoperability 2016
- State Bank of Pakistan: Regulations for Payment Card Security

- State Bank of Pakistan: Regulations for the Security of Internet Banking

Guidelines

- Ministry of Information Technology and Telecommunications: Digital Pakistan Policy 2018
- Ministry of Commerce: E-Commerce Policy of Pakistan 2019
- Ministry of Information Technology and Telecommunications: Pakistan IT Policy Action Plan 2000



Trade Facilitation with Digital Means

This section analyses how well the domestic regulatory environment is set up to welcome goods and services trade made possible through digital tools. This includes the use of electronic trade documentation, as well as measures designed to support "trade in parcels" and streamline cross-border transactions in the digital economy.

Guiding Questions

We analyse whether trade administration documents for imports are available and can be submitted in electronic form. We then focus on single windows, enabling persons to submit documentation for import, export, or transit through a single entry point to authorities. Specifically, we outline whether a single window system is operational for trade documentation and whether this system supports international data or document exchange. Finally, we highlight expedited or simplified customs procedures for low-value shipments.

Pakistan provides electronic trade administration documents and accepts submissions in electronic form. The Single Window Act established the (currently operational) national single window to fulfil import, export, and transit-related requirements in 2021. Subsequent rules specified that operating entities can exchange data with national and international organisations. Finally, simplified customs procedures apply to shipments valued below PKR 5000.

Summary

- The Single Window Act streamlines trade by mandating the submission of import documents on a centralised digital platform and aligns with international standards of data exchange. The Pakistan Single Window Trade Dissemination, Exchange, and Utilisation Rules establish protocols for digital management and sharing of trade data. Moreover, the Pakistan Single Window Integrated Risk Management System Rules streamline trade operations by managing risks electronically and aiding decision-making without the need for physical documents.
- The Pakistan Single Window (PSW) system facilitates cross-border trade through paperless trade integration into the international supply chain, including Pakistan's membership in the Pan-Asian E-commerce Alliance (PAA) and agreements with China, Uzbekistan and Tajikistan. The PSW initiative also includes the integration of the National Plant Protection Organisation (NPPO) integration with the e-Phyto Hub to enable electronic phytosanitary certificates, crucial for international trade. Additionally, the Connectivity with China Single Window (GACC) facilitates paperless data exchange between Pakistan and China to streamline trade operations. Lastly, the Port Community System enhances maritime trade by improving efficiency and supporting paperless trade through digital documentation and streamlined processes.
- The Federal Board of Revenue (FBR), operating under the Ministry of Finance, oversees paperless trade by creating and implementing legislation. The Pakistan Single Window Authority, operating under the FBR, also focuses on paperless trade by providing an automated trade processing platform, integrating regulatory frameworks into trade systems, and imposing penalties for non-compliance.
- The Customs Act calls for an integrated Single Window system, automated compliance checks and electronic communication between traders. The Customs Rules promote paperless trade through the electronic submission and processing of electronic documents. Additionally, Pakistan has a duty de minimis threshold of PKR 5,000 for imports. This means that any product imported through postal or air courier services with a declared value up to PKR 5,000 is exempt from customs duty and other taxes.
- Both the Strategic Trade Policy Framework 2020-25, and the Digital Pakistan Policy 2018, issued by the Ministry of Information Technology and Telecommunication, broadly address paperless trade by encouraging the adoption of electronic systems and digital infrastructure. Additionally, the Pakistan Trade Portal, developed by the FBR, facilitates paperless trade by allowing users to submit and manage trade-related documents online. Furthermore, within the banking sector, the State Bank of Pakistan (SBP) Vision advocates for the development of a digital financial ecosystem and an increased reliance on digital infrastructure.



SOURCES

Primary Legislation

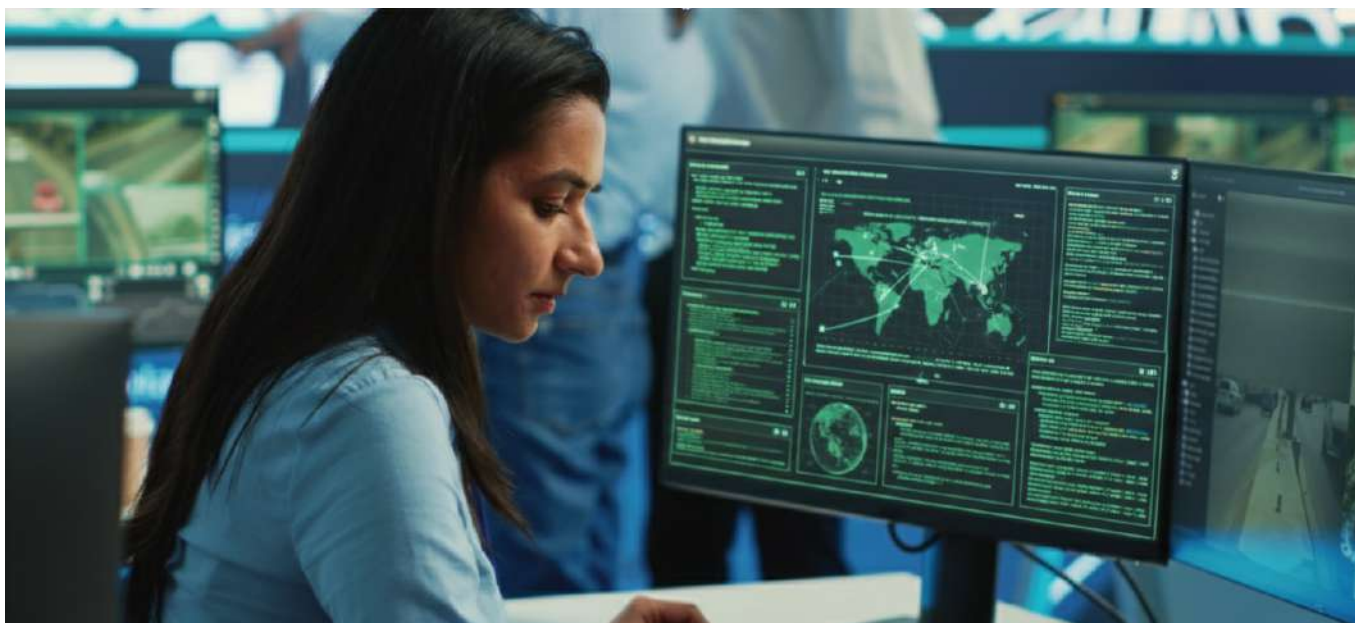
- Customs Act 1969
- Single Window Act 2021
-

Secondary Legislation

- Federal Board of Revenue: Customs Rules 2001 (Amended to 2023)
- Federal Board of Revenue: Pakistan Single Window Integrated Risk Management System Rules 2023
- Federal Board of Revenue: Pakistan Single Window Trade Dissemination, Exchange, and Utilisation Rules 2021

Guidelines

- Ministry of Information Technology and Telecommunications: Digital Pakistan Policy
- Ministry of Commerce: Pakistan Trade Portal (PTP)
- State Bank of Pakistan: SBP Vision 2028
- Ministry of Information Technology and Telecommunication: The Strategic Trade Policy Framework 2020-25
- Federal Board of Revenue: Pakistan Single Window
- GEA - Global Express Association [third party source]



Cybersecurity

This section aims to assess whether the cybersecurity requirements of the member state broadly align with international best practices. While cybersecurity is a critical component of digital policy, its relevance to digital trade is limited. Cybersecurity primarily concerns national defence, critical infrastructure, cybercrime prevention, and system integrity. However, alignment with international cybersecurity standards is essential for creating a secure environment conducive to digital trade. Insufficient cybersecurity standards can undermine trust, while overly stringent requirements may hinder market entry for international service providers.

Guiding Questions

We outline whether there is a regulatory framework regarding cybersecurity. We explain whether this framework is risk-based, creating tiered obligations depending on the extent of cybersecurity risk. We then analyse whether and to whom incident notification is required. Finally, we explain which authority oversees cybersecurity.

The cybersecurity framework comprises a dedicated law on electronic crimes and several other laws and regulations. The framework establishes obligations based on risk levels, for example for critical telecommunications infrastructure, and incident notification requirements. Affected entities must report incidents to the National Computer Emergency Response Team. Licensed critical telecommunications and data infrastructure providers must report incidents to the Telecommunications Authority as soon as possible. Oversight is divided between the Telecommunication Authority and the Computer Emergency Response Team's (at the national, sectoral, and organisational level). The Ministry of Information Technology and Telecommunications oversees and approves cybersecurity policies.

Summary

- The Prevention of Electronic Crimes Act (PECA) serves as Pakistan's primary legislation for addressing cybersecurity. It outlines the legal framework for responding to cyberattacks and curating protective relevant measures. The Pakistan Telecommunication (Re-organisation) Act establishes the standards that telecommunication providers must follow to ensure the cybersecurity of communication networks and protect against unauthorised access of information.
- Since 2023, the Pakistan Computer Emergency Response Team operates under the National Telecom and Information Technology Security Board, which is part of the Pakistan Telecommunications Authority (PTA). It monitors cyber threats, promotes cybersecurity awareness, develops policies and encourages international cooperation by collaborating with international Computer Emergency Response Teams (CERTs). The PTA also implements cybersecurity regulations; ensures the security of communication networks and electronic systems in Pakistan, and imposes penalties and fines for violations. The Federal Investigation Agency collaborates with the PTA and other agencies to investigate and prosecute cybercrimes under PECA. The National Response Centre for Cyber Crime plays a similar role.
- The Computer Emergency Response Team (CERT) Rules manage cybersecurity incidents and establish various specialised CERTs, including the Defence CERT under the Ministry of Defence.
- The Critical Telecom Data and Infrastructure Regulations define critical telecom infrastructure (CTI) and require its identification; classification, and protection. The regulations require comprehensive security measures, including physical security, continuous monitoring, malware protection, and multi-factor authentication. The White Listing of IP Addresses Regulations ensure that only authorised IP addresses are used, bolstering the overall security of telecommunication networks. In the financial sector, the Regulations for the Security of Internet Banking enhance online banking security by mitigating cybersecurity risks associated with digital transactions.
- The National Cybersecurity Policy, issued by the Ministry of Information Technology and Telecommunication (MoITT), promotes active defence measures to protect critical infrastructure and government systems. The idea is echoed in the Pakistan IT Policy Action Plan with an emphasis on securing sensitive information, and in the National Security Policy of Pakistan 2022-2026, with a focus on the wider digital space. Following this, the Access Control Standard Operating Procedure Policy emphasises the importance of securing information assets to ensure authorised access to various cyber spaces. The Internet Usage Standard Operating Procedure safeguards against potential cyber attacks that occur through improper use of the internet.

Additionally, the Data Sharing Standard Operating Procedure mandates strict controls for protecting information by limiting access, prohibiting unauthorised sharing practices e.g. network folder sharing, and classifying data into specific categories with personalised security protocols.



SOURCES

Primary Legislation

- Electronic Transactions Ordinance 2002
- Prevention of Electronic Crimes Act (PECA) 2016
- Pakistan Telecommunication (Re-organisation) Act 1996 Amendments 2006
-

Secondary Legislation

- Computer Emergency Response Team: Rules 2023 (CERT)
- Computer Emergency Response Team: Critical Telecom Data and Infrastructure Security Regulations 2020
- State Bank of Pakistan: Regulations for the Security of Internet Banking
- Pakistan Telecommunication Authority: White Listing of IP Addresses Regulations 2019

Guidelines

- Ministry of Information Technology and Telecommunication: Access Control Standard Operating Procedure

- Ministry of Information Technology and Telecommunication: Internet Usage Standard Operating Procedure
- Ministry of Information Technology and Telecommunication: National Cybersecurity Policy 2021
- National Cyber Emergency Response Team of Pakistan: National Security Policy of Pakistan 2022 - 2026
- Ministry of Information Technology and Telecommunication: Pakistan IT Policy Action Plan 2000

Oversight Authorities

- Federal Investigation Agency (FIA) [source not working]
- National Response Centre for Cyber Crime
- Pakistan Telecommunication Authority (PTA) [source not working]
- The Pakistan Computer Emergency Response Team (PKCERT)



Artificial Intelligence

This section offers an overview of how artificial intelligence (AI) is regulated in the member state. The focus is on the policy response to the rise of widely accessible AI, covering both AI-specific regulatory frameworks and the application of existing laws to AI technologies. From a digital trade perspective, the key consideration is whether the member state aligns with emerging international practices.

Guiding Questions

We outline whether there is a specific regulatory framework addressing AI. If so, we analyse whether the framework is risk-based, meaning it establishes obligations based on the level of AI risk. We also analyse whether the framework is technology-based, meaning it establishes rules based on specific AI technologies. Finally, we reference guidance released by regulatory agencies on how the existing, non-AI-specific framework, applies to AI providers.

There is currently no binding regulatory framework on the governance of AI. Currently, the government is developing the National AI Policy 2024, which aims to establish a legal framework for AI. Pakistan's Digital Policy 2018 mentions the establishment of innovation centres in thematic areas including AI and efforts to build capacity on smart technologies. Regulatory agencies have not issued guidelines on how existing rules apply to AI providers.

Summary

- There is currently no primary or secondary legislation on AI in Pakistan. The Digital Pakistan Policy, issued by the Ministry of Information Technology and Telecommunication (MoITT), promotes the use and development of smart technology, aiming to adopt the Internet of Things, AI and robotics in a cost-effective way. Furthermore, the e-Commerce Policy of Pakistan calls for the integration of AI-driven solutions for more streamlined operations and data analytics.
- Additionally, the MoITT is currently deliberating the National AI Policy (Draft), to establish a legal framework for AI. The policy proposes the creation of an AI Regulatory Directorate (ARD), under the National Commission for Personal Data Protection, to provide support and create further guidelines concerning AI. It also proposes the establishment of a National AI Fund (NAIF) and Centres of Excellence in AI to spearhead research, innovation and skill development.
- Moreover, the Presidential Initiative for AI & Computing (PIAIC), launched in 2018, aims to position Pakistan as a global leader in AI, data science etc, and has leveraged four main programmes focused on these areas to encourage innovation.
- The main authority that oversees artificial intelligence is the MoITT, which formulates national policies; ensures AI integration across all sectors, and imposes fines. The National Information Technology Board operates underneath the MoITT to provide technical support.



SOURCES

Secondary Legislation

- Ministry of Information Technology and Communication: Removal and Blocking of Unlawful Online Content (Procedure, Oversight Safeguards) (Rules 2021)

Guidelines

- Ministry of Information Technology and Telecommunications: Digital Pakistan Policy 2018
- Ministry of Commerce: E-Commerce Policy of Pakistan 2019
- Ministry of Information Technology and Telecommunication: National Artificial Intelligence Policy

2024 (DRAFT)

- President of Pakistan: Presidential Initiative for Artificial Intelligence & Computing (PIAIC)

Oversight Authorities

- Ministry of Information Technology and Telecommunication
- National Information Technology Board (NITB)



Source Code

Source codes are among the essential trade secrets of the digital economy. Potential disclosure requirements toward the government or domestic private companies can be a major hurdle to market access. The purpose of this section is to identify regulatory or enforcement requirements that risk the required disclosure of source code.

Guiding Questions

We explain whether source code is generally protected under the intellectual property framework and whether there are exceptions to this protection. We then identify potential source code sharing requirements, explaining the circumstance and specific software to which they apply. Where explicitly stated, we reference the public policy objective invoked by the government.

The copyright framework protects computer programmes as “literary works”, establishing protections, including reproduction and adaptation rights. The sharing of computer programmes without authorisation is punishable with up to three years of prison or PKR 100’000. Exceptions include fair dealing, such as research and education. Pakistan does not require source code sharing.

Summary

- The Copyright Ordinance covers computer programmes as “literary works”, establishing protections, including reproduction and adaptation rights. The Ordinance further establishes penalties for sharing computer programmes without authorisation. The Ordinance outlines various acts that do not constitute copyright infringement, including fair dealing for research, news reporting, and educational purposes, among others. The Copyright Rules specify the legislation, granting copyright protection against unauthorised reproduction and distribution of the computer program.

Pakistan does not require mandatory source code sharing.



SOURCES

Primary Legislation

- Copyright Ordinance 1962 (No. XXXIV of 1962) [other government source]
- The International Copyright Order 1968 [other government source]

Secondary Legislation

- Intellectual Property Organisation of Pakistan: The Copyright Rules 1967 [source not working]



Digital Economy Taxation and Customs Duties

The purpose of this section is to identify how the digital economy is taxed domestically and at the border. This covers direct taxes, indirect taxes, and customs duties, applicable to both digital services/products and e-commerce imports. We focus on whether a) requirements are applied identically to digital services/products as to their analog equivalents and b) requirements are applied identically to domestic and foreign suppliers.

Guiding Questions

We explain whether customs duties apply to digital services/products as well as e-commerce imports. We then analyse whether indirect taxes, such as value-added-tax, apply to digital services/products as well as e-commerce imports. In addition, we identify any direct taxes imposed specifically on providers of digital services/products, such as digital service taxes. For each tax or duty, we mention whether electronic registration is possible for foreign providers.

Digital services and digital products are not subject to customs duties but are subject to the sales tax. E-commerce imports are subject to both customs duties and sales tax. Pakistan further levies a direct tax on providers of digital services or digital products. The “fee for offshore digital services” targets online advertising, website and content hosting, as well as e-commerce providers and levies a fee on royalties paid from Pakistan. Electronic tax registration is possible.

Summary

- The Customs Act applies customs duties on certain imported goods, including e-commerce imports. The Customs Rules, amended in 2020 and 2021, regulate customs procedures for all imports, including e-commerce. The 2021 amendment specifically creates tailored customs procedures for e-commerce imports and exports, detailing responsibilities for paying customs duties.
- The Sales Tax Act regulates the imposition, collection and management of the 18% sales tax. The Finance Act amends the Sales Tax Act and applies a 2% tax on the gross value of supplies for online marketplaces, including e-commerce platforms. The Sales Tax Rules 2006 outline the procedure for administering and collecting the sales tax, without specifically addressing customs duties or e-commerce imports.
- Furthermore, under the Income Tax Ordinance, a Digital Services Tax (DST) is levied on non-resident entities receiving payments from Pakistan for certain digital services, including on royalties and fees for offshore digital services, payment operations and technical services. This includes services such as digital advertising, the designing, creating, hosting or maintenance of websites, the hosting of websites, computing, blogs, online content and online data, the collection or processing of data of users in Pakistan, and the facilitation of online sales of goods or services. The DST is calculated on the gross amount of these receipts at a rate of 15% for non-resident entities that do not have a permanent establishment in Pakistan. Furthermore, the Ordinance imposes a tax of 0.25% on the total sales revenue of online businesses in



Pakistan, including e-commerce sellers and marketplace operators, irrespective of their reported profits. This minimum tax applies to all businesses operating in the digital economy.

- Previously, the e-Commerce Policy of Pakistan highlights the need for clarity with regards to customs duties and indirect taxes on digital goods and services, and advocates for simplified tax compliance and the consideration of a direct tax on digital service providers.
- The Financial Board of Revenue is responsible for overseeing federal taxes. However, regarding sales tax on digital services, provincial revenue authorities such as the Punjab Revenue Authority), Sindh Revenue Board, Khyber Pakhtunkhwa Revenue Authority), and the Balochistan Revenue Authority are tasked with oversight.



SOURCES

Primary Legislation

- Customs Act 1969
- Finance Act 2021
- Sales Tax 1990 (amended to 2024)
- Income Tax Ordinance 2001 (amended to 2023)

Secondary Legislation

- Federal Board of Revenue: Sales Tax Rules 2006 (amended to 2023)
- Federal Board of Revenue: Customs Rules 2001 (amended in 2020)
- Federal Board of Revenue: Customs Rules 2001 Amendment 2021
- Directorate for Services rendered and repealing the previous text

Guidelines

- Ministry of Commerce: E-Commerce Policy of Pakistan 2019

Oversight Authorities

- Balochistan Revenue Authority (BRA) [source not working]
- Federal Board of Revenue (FBR)
- Khyber Pakhtunkhwa Revenue Authority (KPRA)
- Punjab Revenue Authority (PRA) [source not working]
- Sindh Revenue Board (SRB)



Electronic Payments

This section evaluates the key aspects of the regulatory environment governing electronic payments and its openness to processing payments across borders. Electronic payments are a critical enabler of digital and digitally facilitated trade. While data protection, data flows, and electronic transactions play a significant role in electronic payments, they have been addressed previously. This section focuses on whether a) digital payment services/products are subject to the same requirements as their analogue equivalents, and b) whether these requirements are applied equally to domestic and foreign providers.

Guiding Questions

We outline whether there is a regulatory framework specifically addressing electronic payments. We then distil know-your-customer, anti-money-laundering, and counter-terrorism-financing rules that apply to electronic payments. In addition, we delineate licensing requirements and procedures for entities that offer electronic payment services. Finally, we reference special regulatory requirements for cross-border electronic payments.

Digital payments are governed by the general regulatory framework for payments, which have specific rules for electronic funds transfers. Accordingly, general know-your-customer, anti-money-laundering, and counter-terrorism-financing rules apply to digital payments. In addition, payment system operators and payment service providers (including e-commerce gateways) must receive a licence from the central bank. No specific rules apply to cross-border payments.

Summary

- Electronic payments are governed by several laws. The Payment Systems and Electronic Fund Transfers Act requires electronic payment providers to obtain licences and uphold know-your-customer (KYC), anti-money-laundering (AML), and counter-terrorism-financing (CTF) rules. The Anti-Money Laundering Act 2010 sets out a general framework of KYC, AML, and CTF rules. Recent amendments impose more stringent due diligence requirements on digital payment operators, and suspicious activities are to be reported to the Financial Monitoring Unit.
- The State Bank of Pakistan is the main body responsible for digital payments. It issues regulations and guidance, ensures compliance with AML and KYC rules and issues licences to payment service providers. The SBP's Regulations specify due diligence and licensing requirements. Moreover, the Electronic Fund Transfer Regulations mandate identity verification processes and risk management strategies in line with anti-terrorism financing aims and outline the role of Payment System Operators and Payment Service Providers.



The Digital Pakistan Policy, issued by the Ministry of Information Technology and Telecommunication, promotes compliance with international AML, KYC and CFT standards and advocates for a national e-payment gateway to facilitate cross-border digital payment transfers. Lastly, the Foreign Exchange Regulation Act regulates digital exchange channels.



SOURCES

Primary Legislation

- Anti-Money Laundering Act 2010 (Amendment 2020)
- Anti-Money Laundering (Amendment) Act 2015
- Anti-Money Laundering (Amendment) Act 2020
- Foreign Exchange Regulation Act (FERA) 1947 Act No. VII of 1947
- Payment Systems and Electronic Funds Transfers Act 2007

Secondary Legislation

- State Bank of Pakistan: Electronic Fund Transfers (EFT) Regulations 2018 Modalities for the exercise of the activities of Electronic Money Issuers and Distributors

Guidelines

- Ministry of Information Technology and Telecommunications: Digital Pakistan Policy 2018
- State Bank of Pakistan: National Financial Inclusion Strategy (NFIS)



SMEs and Digital Inclusion

Digital trade holds the potential to open global markets to SMEs and disadvantaged groups. By leveraging digital technologies, small businesses, rural enterprises, and minority-owned businesses can overcome traditional barriers to international trade, such as high costs, limited market access, and logistical challenges. E-commerce platforms, digital payment systems, and online marketing tools enable these businesses to reach international customers, integrate into global value chains, and attain economies of scale previously limited to larger corporations. This section highlights recent support measures targeted to helping SMEs and disadvantaged groups capitalise specifically on the opportunities of the global digital economy.

Guiding Questions

We analyse whether the government has established specific programs or initiatives to support SMEs or disadvantaged groups in participating in the digital economy or digital trade. For each program, we distil the objective of the support, the form of support provided, and the target group of the program.

Pakistan has implemented several policy initiatives and programmes to support SMEs and disadvantaged groups in leveraging digital trade opportunities. These measures include the development of a national e-commerce policy, strategic frameworks targeting SME participation in digital marketplaces, and collaborative efforts between government agencies to enhance SME capacity for digital exports. The initiatives encompass a range of services, from technical and financial assistance to digital skills development and market linkages.

Summary

- The 2018 Digital Pakistan Policy establishes a foundational objective to integrate Micro, Small and Medium Enterprises (MSMEs) and disadvantaged groups into online commerce activities. This policy sets the stage for subsequent, more targeted initiatives. Building on this, the E-commerce Policy of Pakistan, announced in October 2019 by the Commerce Division, outlines specific goals and support mechanisms. These include facilitating the entry of 50,000 SMEs into online marketplaces, developing an e-commerce information hub for new businesses, and promoting e-commerce exports among SMEs. The policy also aims to connect SMEs with global online platforms through digital marketing and collaborate with organisations to improve SME access to finance for e-commerce activities.
- The Strategic Trade Policy Framework 2020-2025 further reinforces the government's commitment to digital inclusion for SMEs. It specifically focuses on linking small and medium private sector entrepreneurs at the retail level with e-commerce opportunities, indicating a continued emphasis on integrating SMEs into the digital economy.
- To implement these policy objectives, government agencies have established collaborative programmes. In September 2020, the Small and Medium Enterprises Development Authority and the Trade Development Authority of Pakistan signed a three-year agreement. This initiative targeted SMEs and women entrepreneurs, offering technical and financial assistance, support for digitisation, and facilitation of market linkages abroad via e-commerce platforms.
- More recently, the Trade Development Authority of Pakistan introduced the Pakistan Trade Portal, as reported at the 9th National eCommerce Council meeting on 28 May 2024. This portal serves as a capacity-building platform for e-commerce, registering several thousand buyers, sellers and products across the country. While not exclusively limited to SMEs, this initiative provides a digital infrastructure that can benefit small businesses seeking to expand their market reach.
- The government has also implemented measures to address specific barriers faced by SMEs and freelancers in digital trade. These include enhancing monthly earning limits for freelancers and facilitating small packet e-commerce exports.



SOURCES

- Trade Development Authority of Pakistan: Strategic Trade Policy Framework 2020-2025
- Ministry of Information Technology and Telecommunications: Digital Pakistan Policy
- Ministry of Commerce: E-Commerce Policy of Pakistan
- Trade Development Authority of Pakistan: Memorandum of Understanding between TDAP and SMEDA
- Trade Development Authority of Pakistan: 9TH NATIONAL ECOMMERCE COUNCIL MEETING



02

Digital Economy Factsheet

Digital Economy Factsheet

This factsheet describes Pakistan's digital economy across four key dimensions: digital economy size and activities, digital infrastructure and connectivity, digital skills, and digital government.



Size and Activities of the Digital Economy

To describe the size and activities of Pakistan's digital economy, we used data provided by the World Trade Organization and conducted our own calculations. We specifically analyzed the share of advanced technology products in total trade, cross-border trade in telecommunications, computer, information and audiovisual services, and total digitally delivered services..

Advanced technology products accounted for 7.88% of Pakistan's imports. The share of advanced technology products in exports was lower at 1.85%, indicating a technology trade imbalance.

Figure 1:
Telecommunications, Computer, Information and Audiovisual Services.

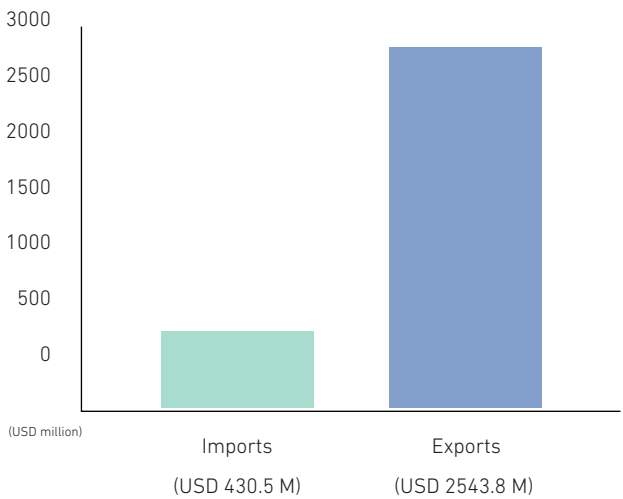


Figure 1 provides data for Pakistan's telecommunications, computer, information, and audiovisual services in 2022.

Figure 2:
Digital Delivered Services

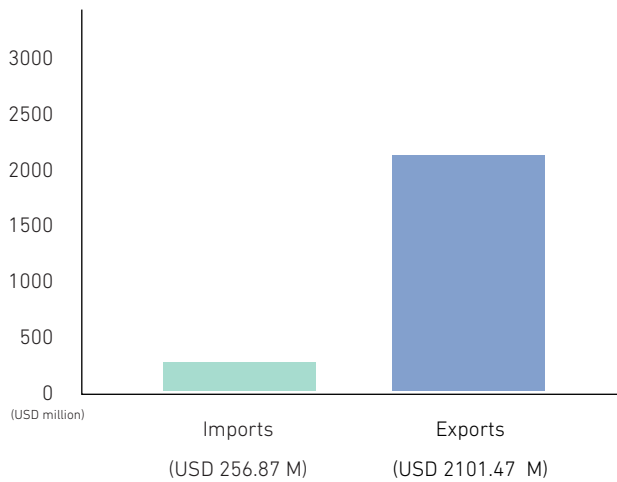


Figure 2 provides data for the total digitally delivered services in 2023.

Digital Infrastructure and Connectivity

To analyze Pakistan's digital infrastructure and connectivity, we analyzed data provided by the International Telecommunications Union. We focused on internet access, broadband coverage, and traffic, as well as mobile phone ownership..

Figure 3:
Digital Infrastructure and Connectivity

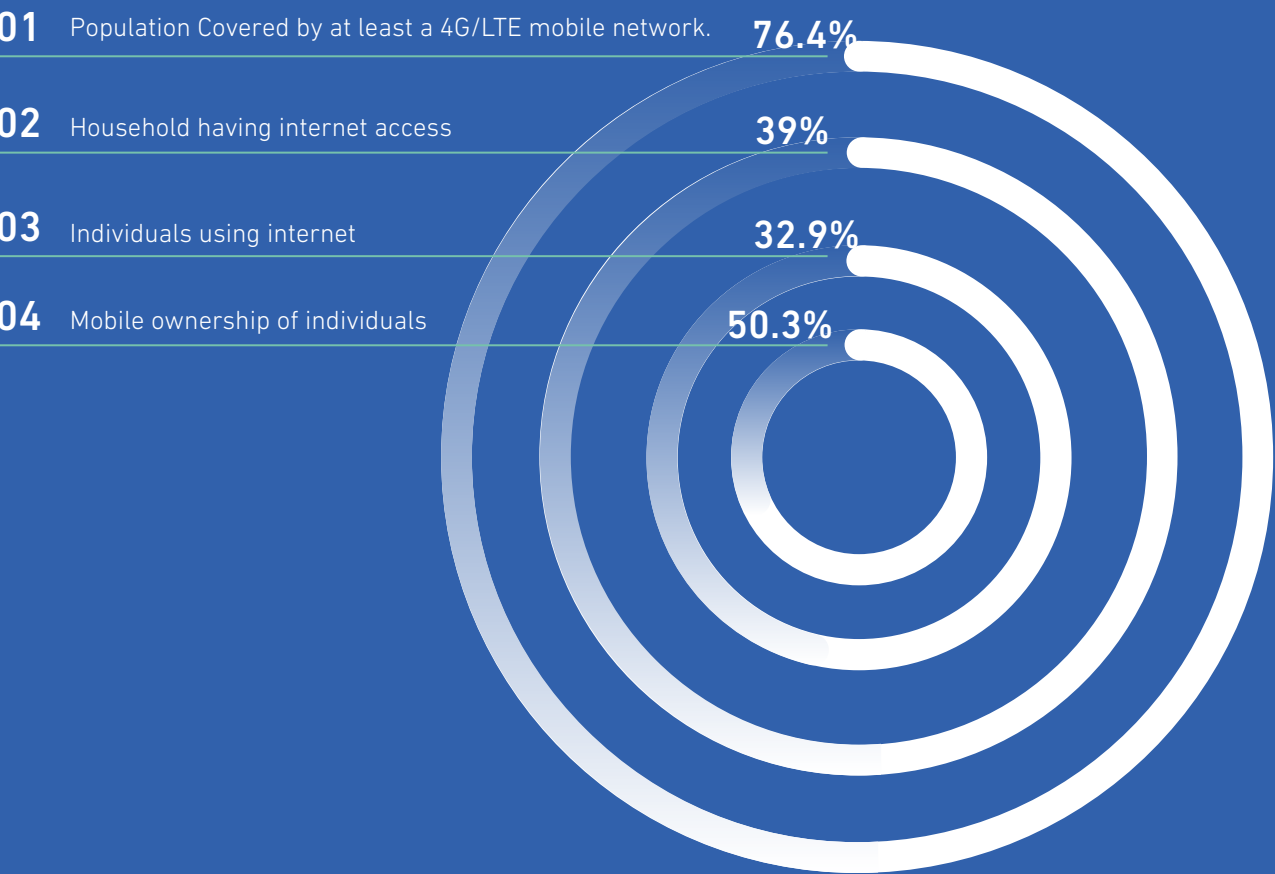


Figure 3 provides data to analyze Pakistan's digital infrastructure and connectivity in 2022.



Digital Skills

To document Pakistan's digital skills, we draw on data by UNESCO. We use data points relevant to digital skills, beginning with general education and moving to specific digital skills.

The upper secondary education completion rate in Pakistan was 14.84% in 2007. Gross tertiary education enrollment ratio stood at 11.22% in 2023, indicating relatively low participation in higher education. The adult literacy rate was 58% in 2019. Government expenditure on education as a percentage of GDP was 4.2% in 2022.

The proportion of youth and adults with basic digital skills in Pakistan showed low competency levels:



5.12%

were able to copy or move a file or folder (2019)



1.58%

had created electronic presentations with presentation software (2020)



2.41%

could find, download, install and configure software (2020).



Digital Government

To examine the state of digital government in Pakistan, we rely on the World Bank's GovTech dataset. Specifically, we analyze how Pakistan provides digital government services, establishes institutions, and drafts strategies.

In terms of digital government services in 2022, Pakistan had only a cloud strategy/policy with no platform yet. It did not have a government interoperability framework. It did not have a government open-source software policy or action plan. Pakistan did not maintain an open government portal or an open data portal.

Regarding institutional frameworks for digital government in 2022, Pakistan had established a government entity focused on government technology or digital transformation. It had established a government entity focused on public sector innovation. Pakistan had a whole-of-government approach to public sector digital transformation in draft or planned.

Finally, Pakistan had drafted various strategies to advance digital government in 2022:

- 01 It had a current government technology or digital transformation strategy
- 02 It had either a strategy or program to improve digital skills in the public sector
- 03 It had either a strategy or program to improve public sector innovation



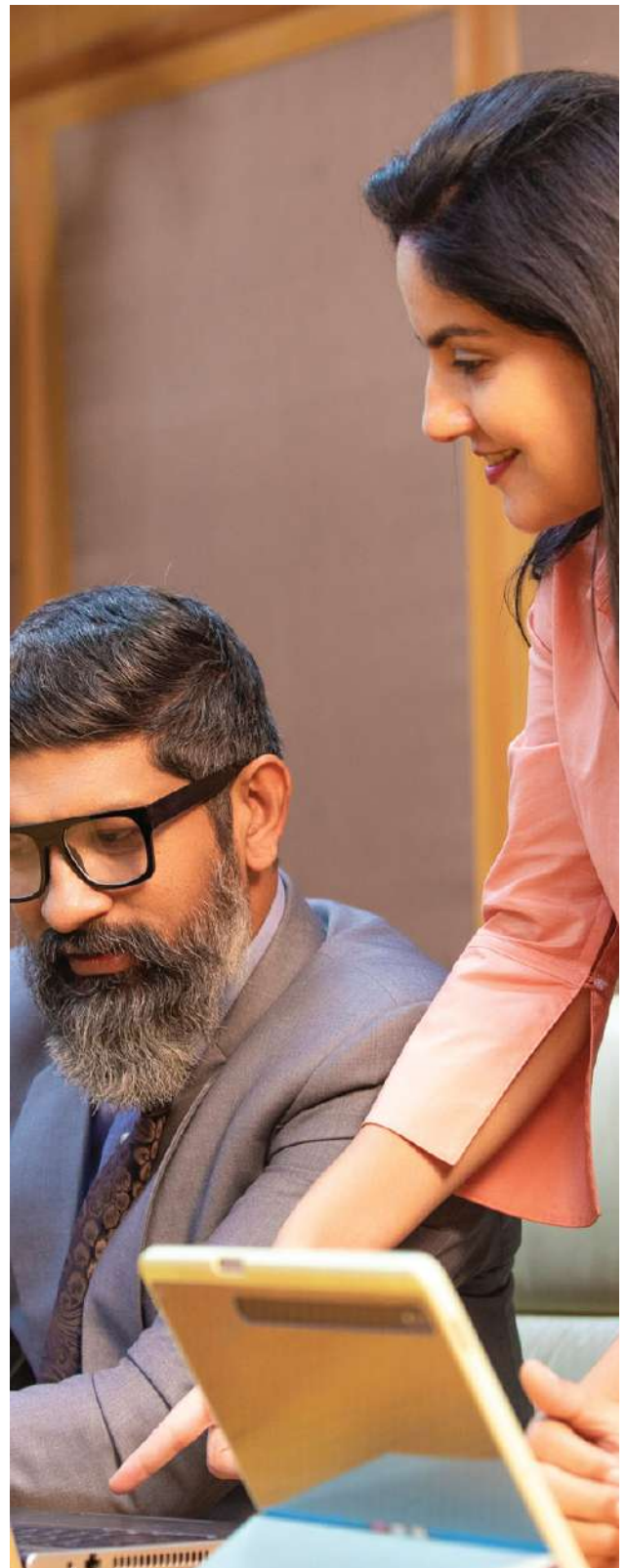
03

International Commitments and Collaboration

International Commitments and Collaboration

The purpose of this section is to outline the existing international commitments of Djibouti and explain in which fora it engages in. We focus on international commitments and collaboration with a digital component, meaning a connection to the pertinent policy areas explained above.

To outline international commitments, we analyse binding free trade agreements and conventions, as well as non-binding guidelines/recommendations/principles and model laws. We also reference other commitments, both binding and non-binding. For each commitment, we explain whether it is binding and which policy area(s) it can impact. Regarding international fora, we analyse participation in discussions at the pluri- and multilateral level.





Commitments

Free Trade Agreements

Pakistan has not signed any free trade agreements, which include provisions related to digital trade.

Conventions

Pakistan is party to the following conventions and agreements:

- 01 International Covenant on Civil and Political Rights (Data Protection)
- 02 G20/Organisation for Economic Co-operation and Development Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting (Taxation)
- 03 Berne Convention for the Protection of Literary and Artistic Works (Source Code)

Guidelines, Recommendations, and Principles

Pakistan is a member state of the United Nations, which has adopted the following frameworks:

- 01 United Nations Guidelines for Consumer Protection (Online Consumer Protection)
- 02 United Nations Educational, Scientific and Cultural Organization Recommendation on the Ethics of Artificial Intelligence (Artificial Intelligence)
- 03 United Nations draft Resolution A/78/L.49 on Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development (Artificial Intelligence)

Models

Pakistan is a member state of the United Nations, which has adopted the following frameworks:

- 01 United Nations Commission on International Trade Law Model Law on Electronic Commerce (Electronic Transactions)
- 02 Commonwealth Model Law on Computer and Computer Related Crime (Cybersecurity)
- 03 Commonwealth Model Provisions on Data Protection (Data Protection)

Other Commitments

● Pakistan is a member of the World Trade Organization and as such is subject to the Moratorium on Customs Duties on Electronic Transmissions (Customs Duties), the Trade Facilitation Agreement (Trade Facilitation) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (Source Code).

Pakistan is a member of the International Organization for Standardization, which has issued various technical standards including:

- 01 ISO/IEC 22989:2022 (Information technology — Artificial intelligence — Artificial intelligence concepts and terminology) (Artificial Intelligence)
- 02 ISO/IEC 42001:2023 (Information technology — Artificial intelligence — Management system) (Artificial Intelligence)
- 03 ISO 22376:2023 (Security and resilience — Authenticity, integrity and trust for products and documents — Specification and usage of visible digital seal data format for authentication, verification and acquisition of data carried by a



- document or object) (Cybersecurity)
- 04 ISO 31700-1:2023 (Consumer protection — Privacy by design for consumer goods and services) (Consumer protection)
- 05 ISO 13491-1:2024 (Financial services — Secure cryptographic devices (retail) (Cybersecurity)
- 06 ISO/TS 23526:2023 (Security aspects for digital currencies) (Cybersecurity)
- 07 ISO 23195:2021 (Security objectives of information systems of third-party payment services) (Electronic payments)
- 08 ISO 32111:2023 (Transaction assurance in E-commerce — Principles and framework) (Electronic transaction)

Fora

Pakistan participates in the United Nations Global Digital Compact (Cross-cutting).



○ The Critical Telecom Data and Infrastructure Security Regulation, which demands the localisation of critical telecom data, including personal data related to licensees and customers, for example voice and communication data;

The Data Retention of Internet Extended to Public WiFi-Hotspots Regulations, which demands the localisation of data from public WiFi spots; and

The Telecom Consumers Protection Regulations, which requires data related to consumer interactions and transactions to be localised.

○ In the financial sector, several localisation mandates apply:

The Anti-Money Laundering Act mandates that financial institutions store and process their data within national borders.

The Payment Systems and Electronic Fund Transfers Act and its Regulations state that e-payments and associated transactions must be managed domestically for better oversight.

The Regulations for Technical Implementation of Mobile Banking also mandate localisation.

○ Furthermore, the proposed Personal Data Protection Final Draft Bill would mandate that critical data must always be processed and stored on servers within Pakistan, subject to approval from authorities. Transfers of other types of personal data would only be allowed if the recipient provides adequate data protection measures (see section on Cross-Border Data Transfers above).

The Pakistan Telecommunication Authority oversees the telecommunications sector, issuing licences enforcing compliance and leading legal investigations.

- The Protection from Spam, Unsolicited Fraudulent and Obnoxious Communication Regulations contain provisions regulating the dissemination of spam, fraudulent messages and other forms of unwanted communication. The Telecom Consumers Protection Regulations govern consumer protection in commercial practices, punishing misleading or false advertising. The 2016 amendment establishes consumer complaint mechanisms and emphasises transparency in information. The Ministry of Commerce's E-Commerce Policy aims to create a broad framework for regulating e-commerce, including consumer protection mechanisms.

