Policy Research Working Paper 9199

Digital Trade in MENA

Regulatory Readiness Assessment

Lillyana Daza Jaller
Martín Molinuevo

WORLD BANK GROUP
Middle East and North Africa Region
Office of the Chief Economist
&
Macroeconomics, Trade and Investment Global Practice
March 2020

Abstract

A strong regulatory framework can provide essential tools for remote transactions and improve trust in digital trade. Yet, regulations can also introduce restrictions that hamper the conditions for digital markets. Based on a database of 20 Middle East and North Africa countries and 20 comparator countries around the world, this paper shows that the Middle East and North Africa region is falling behind in establishing a modern governance framework for the digital economy. The analysis focuses on a set of regulatory areas, including electronic documentation and signature, online consumer protection, data governance, cybersecurity, and intermediary liability regulations. It assesses each country's domestic regulatory framework in light of recent international trends and regulatory models. The study shows that regulation of digital markets in countries in the region is still in its infancy, being mostly governed by general laws that were not originally intended for the digital era. Some countries have tried to support an export-oriented information technology sector by keeping an updated regulatory framework. However, regulation in most countries in the region, regardless of their level of development, still features some major loopholes that can limit consumer trust in digital markets or reduce certainty—and increase costs—for digital businesses.

This paper is a product of the Office of the Chief Economist, Middle East and North Africa Region and the Macroeconomics, Trade and Investment Global Practice. . It is part of a larger effort by the World Bank to provide open access to its research and make a contribution to development policy discussions around the world. Policy Research Working Papers are also posted on the Web at http://www.worldbank.org/prwp. The authors may be contacted at mmolinuevo@worldbank.org.

Digital Trade in MENA

Regulatory Readiness Assessment

Lillyana Daza Jaller
Martín Molinuevo

JEL Codes: F13, K24, L86, O38

Keywords: e-commerce, digital markets, regulatory framework, data policy

This note was prepared by Lillyana Daza Jaller (Consultant), and Martín Molinuevo (Senior Counsel, ETIRI), as a background paper for a World Bank study on "*New Economy Agenda for MENA*", under the guidance of Antonio Nucifora (Manager). The authors are grateful to Daniel Lederman, Martha Licetti, Ana Paula Cusolito, Christina Wood, Francois De Soyres, Jerome Bezzina, and the participants to the author's workshop of July 2019 for valuable comments and suggestions.

This note was partially funded by the Umbrella Facility for Trade Trust Fund (UFT), established with contributions from DFID, Sida, SECO, the Netherlands Ministry of Foreign Affairs, and the Norwegian Ministry of Foreign Affairs.

Digital Trade in MENA

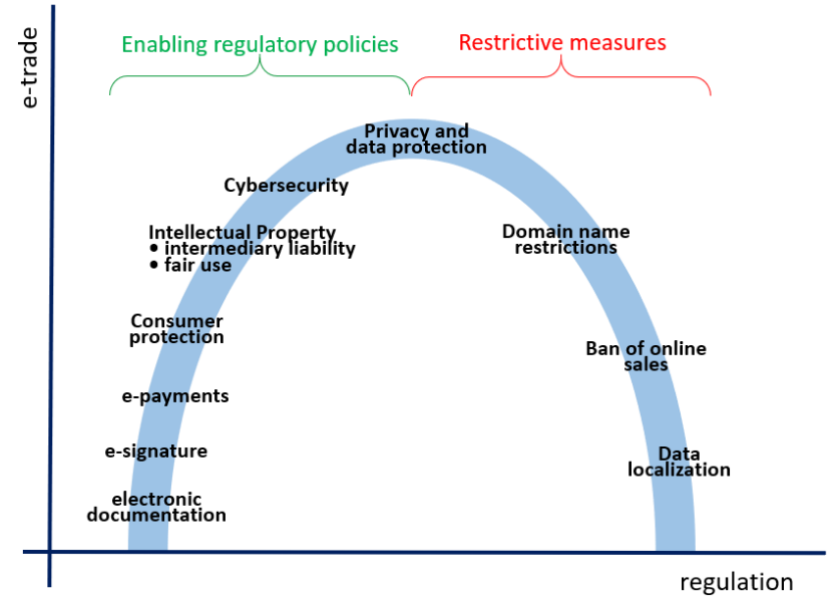
Regulatory Readiness Assessment

I. Introduction

Regulation plays a central role in building the foundations of digital markets. It can provide the legal tools necessary for remote contracts, clarify the rights and obligations of the multiple actors involved in digital transactions, and establish a framework that promotes consumer trust in digital markets, even when the consumer does not know the merchant or when the merchant is in a different country.

The regulation of digital markets is a patchwork of regulatory solutions from different policy areas. Broadly speaking, the regulation of e-trade entails elements of contract law, particularly with regards to electronic documents and signatures, as well as laws related to consumer protection, intellectual property, cybersecurity, personal privacy, and data protection. A conducive regulatory framework in each of these policy areas is necessary for vibrant digital markets. However, specific restrictive measures within these areas may undermine e-trade, for example by unnecessarily curbing the types of goods that can be traded remotely or by limiting the cross-border flows of data that underpin e-trade transactions.

Figure 1: Domestic regulation can either foster or hinder e-trade



Laws and regulations can hence either foster or hinder digital trade (Figure 1). Regulation can play three different roles for digital markets. First, it can provide essential regulatory tools for remote transactions, such as electronic documents and signatures; Second, it can improve the conditions for trust in digital markets, by ensuring that consumers are protected, and that their information is safe and remains private, hence increasing reliance and bringing new actors to digital transactions. A strong regulatory framework on these aspects can be associated with the expansion of digital trade – represented on the upward part of the slope in Figure 1. Yet, third, regulations can also introduce restrictions that hamper the conditions for digital markets, by restricting the types of goods and services that can bought online; by limiting or increasing costs for the transfer of data—which is necessary for the transactions—or creating burdensome conditions for online marketplaces, platforms, and services providers, which ultimately limits the offer of goods and services in digital markets.

Regulation of digital markets in Middle East and North Africa (MENA) countries is underdeveloped, being mostly covered by general laws not originally intended for the digital era. Regulations on long-standing digital policies, such as e-documents and e-signatures, are found throughout the region, but even those frameworks are largely outdated and incomplete. Only a handful of countries have advanced in most key regulations for digital markets, but comprehensive and up-to-date regulatory solutions are only found in a few countries in the region, notably Qatar, Bahrain, and Morocco, while others, like Lebanon and Tunisia, also provide comprehensive regulations, albeit with small gaps. Digital regulation is virtually inexistent in a few countries like Iraq, Jordan, UAE, and Kuwait, whose frameworks are severely outdated (in areas like electronic transactions) or stemming from broader frameworks not designed for current digital markets (on data governance and intermediary liability). For a quick attempt to catch up on digital regulations, these countries could adopt the approach of Lebanon, which recently introduced a law on e-commerce tackling multiple regulatory policies at once, from e-signature to intermediary liability. Most countries in the region, including Lebanon, as well as Oman, Jordan, the Islamic Republic of Iran, and UAE would benefit from detailed, specific regulations to expand the broad frameworks already in place, as well as new frameworks to address current gaps.

A. Approach and methodology

In what follows, this study reviews the main policy areas that build the regulatory framework for digital markets for countries in the MENA region. The study considers a set of regulatory areas of central importance to digital markets and assesses the domestic regulatory frameworks in light of recent international trends and regulatory models. In particular, the study addresses electronic documentation and signature; online consumer protection; data governance; cybersecurity; and intermediary liability regulations.

To guide the analysis, the study draws on a pilot database for regulation on digital trade in 40 countries.[1] The data are based on the review of laws and regulations relating to electronic documentation and signature; online consumer protection; data governance; cybersecurity; and intermediary liability regulations in MENA countries as well as over 20 comparator countries. This provides information on the regulatory stances of the different countries on a selected set of key provisions relevant to trade policy. At the same time, the codification of the regulatory frameworks allows to translate that regulatory information into dummy variables or into a Digital Trade Regulatory Readiness Index to be used in economic analysis.

The study offers an overall assessment of how comprehensive and up to date the regulatory framework for digital trade is. The different regulatory areas under review have in common that, taken together, they offer a set of basic rules that create tools for remote transactions (e-document and e-signature) or clarify conditions of digital transactions that enhance consumers' (online consumer protection; data governance and cybersecurity) and business' (intermediary liability) trust. Importantly, however, there are a number of additional policies relevant to digital trade that are not covered in the current study: regulations related to competition policy, taxation, e-payments, as well as the conditions for business licenses, which can also make or break a conducive framework for digital businesses.

[1] See Annex 1 for details.

In assessing these regulatory fields, the analysis focuses on selected regulatory options within each of these fields, so as to assess the regulations in the region in a comprehensive manner. For example, when assessing e-signature regulation, the study discusses the scope of the signature and legal validity given to the e-signature. While an in-depth assessment of the regulation of e-signature in a specific country would require discussing several other aspects that are referenced only in passing in this analysis (e.g. the nature of the certifying provider), the assessment of these key regulatory options provides a picture of the level of sophistication of the regulation and its timeliness in keeping with the policy challenges introduced by digital transactions.

The different sections of the study are focused on the different regulatory fields under consideration, and a concluding section summarizes the main findings and offers policy recommendations. Each section first presents the key features of the regulation and highlights international regulatory practices and models and then describes the regulatory practices by MENA countries in that particular area, assesses strengths and weaknesses of the regulations, and provides recommendations.

II. Regulation on electronic transactions

The legal recognition of electronic documents and signatures as adequate tools for remote businesses is a key step in building a thriving digital market. As communication technologies connect people and businesses around the world with increasing ease and convenience, businesses engaged in digital trade also expand their network of clients and suppliers across borders. A conducive regulatory framework for digital trade should hence guarantee that contracts concluded remotely through electronic channels are valid and legally enforceable just as those concluded in person. Ensuring that electronic documents and signatures are fully recognized and can be enforced is therefore an essential regulatory step to allow for remote electronic contracts and transactions.

Being a key enabler for cross-border businesses, the regulation of electronic transactions is one of the few areas of digital regulation with dedicated international guidance and substantive regulatory experience around the world. In fact, regulation on electronic information and signatures can be traced back to the use of the telegraph in the 19th century.

All countries in MENA have advanced on regulating electronic transactions, typically following the United Nations Commission on International Trade Law (UNCITRAL) guidelines for e-documents and e-signatures. Nonetheless, most regulatory frameworks remain incomplete or outdated, providing partial solutions (e-documents) or unnecessarily burdensome requirements that limit the use of electronic transactions (e-signatures). In the case of e-signatures, it also remains unclear whether MENA countries have established the institutional setting necessary to support e-signature regulation, which undermines the regulation itself.

A. Electronic documentation

A strong and reliable framework for e-documents is particularly important for business-to-business (B2B) transactions. Transactions by final consumers, such as those on e-commerce platforms like Souq.com and app-based services like Airbnb, do not typically entail major documentation exchanges and can be concluded even without a specific regulatory framework for electronic transactions. However, for business relations that require a degree of customization of the products and services and that are provided over time, such as those that allow suppliers to

connect to global value chains and/or services that require peripatetic delivery over extended contract periods, the ability to conclude a contract or amend its terms remotely in a secure and reliable manner is a key step towards engaging in business-to-business digital trade.

International guidelines and practice

UNCITRAL Model Law on Electronic Commerce (MLEC) of 1996 is the international standard on regulation of electronic documents. The main objective of the MLEC is to facilitate remote transactions by establishing rules to allow the electronic equivalent of paper-based documents to be legally recognized, thereby removing obstacles to remote transactions. The MLEC promotes the principles of non-discrimination, technological neutrality, and functional equivalence in the treatment of electronic documentation. The principle of non-discrimination is the cornerstone of the regulation, as it ensures that a document would not be denied legal effect, validity, or enforceability solely on the grounds that it is in electronic form.

Regulation can recognize the validity of electronic documents in general terms or provide specific provisions on key regulatory issues. All regulations inspired in the MLEC at very least ensure the legal validity of documents can be recognized and enforced, even when found in electronic form. Specific regulations on electronic documents further elaborate and provide answers on specific uses of e-documents, such as evidential weight and technological neutrality. Specific rules on electronic documents that tackle issues like evidential weight and technological neutrality, and most often both such elements, are clearly the preferred type of regulation in the selected comparator countries (Table 1). While most of these countries have technologically neutral provisions in their e-document regulation, several – mainly those located in Central and South Asia—lack provisions recognizing the evidential weight of e-documents.

Table 1. Adoption of domestic regulation on e-documents

	E-Docs regulation			
	None	General	Specific	
			Evidential weight	Technological neutrality
Albania			•	
Armenia				•
Bangladesh				•
Burkina Faso			•	•
Canada			•	•
Colombia			•	•
France			•	•
Honduras			•	•
Indonesia			•	•
Kazakhstan		•		
Kenya				•
Korea, Rep.				•
Kyrgyzstan		•		
Malaysia				•
Mexico			•	•
Moldova			•	•
Pakistan				•
Senegal			•	•
Tanzania			•	•
Vietnam			•	•

Specific rules on e-documents address the issue of the evidential weight of electronic documents when presented as evidence in legal proceedings. The MLEC provides that e-documents should not be denied admissibility as evidence in legal proceedings solely based on their electronic nature. The probative value of an e-document should be assessed based on several factors, including the reliability of the methods used for creation, storage, and transmission.

Technologically neutral regulation grants parties to an online transaction the freedom to choose the adequate technology based on their needs. Additionally, certain laws include requirements regarding the way e-documents are stored, such as requiring encryption, which can be unduly

restrictive. In that sense, it is worth recalling that any type of electronic communication, including through casual means like text messages, emails, or electronic chat, can be considered an electronic document with probative value, even when such communications are not encrypted or are relative weak in cybersecurity terms. According to the MLEC, a requirement to store an e-document unaltered is inappropriate, as data messages tend to be decoded, compressed, or converted in the storage process. The MLEC provides the following conditions for the storage of e-documents:

- The information must be accessible for subsequent reference;
- The information must be stored in the manner in which it was created or transmitted, or in a manner which can be demonstrated to accurately represent it; and
- Any existing information that enables the identification of the origin and destination of the data message and the data and time of transmission must be stored.

MENA

All MENA countries, except for Djibouti and the Republic of Yemen, have adopted regulations that recognize electronic documents as equivalent to paper-based documents (Table 2). Israel has done so by including provisions recognizing the general principal of non-discrimination of e-documentation in its legislation on electronic signature. The rest of the countries in the region have instead adopted a more developed framework on e-documents, reflecting in greater detail the principles of the UNCITRAL MLEC. While a more detailed regulation offers advantages in terms of clarity of the regulation, both approaches do give legal recognition to electronic documents.

Table 2. Adoption of regulation on e-documents in MENA

	E-Docs regulation			
	None	General	Specific	
			Evidential weight	Technological neutrality
Algeria			•	•
Bahrain			•	•
Djibouti	•			
Egypt, Arab Rep.			•	
Iran, Islamic Rep.			•	
Iraq				•
Israel		•		
Jordan			•	•
Kuwait			•	
Lebanon			•	
Morocco			•	•
Oman			•	•
Qatar			•	•
Saudi Arabia			•	•
Tunisia			•	•
United Arab Emirates			•	•
Yemen, Rep.	•			

Lebanon was the last MENA country to recognize electronic documents, with a broad e-transaction law entering into force in October 2018. While it is recognized that new law comes to fill an important vacuum, the law has received substantial criticism.[2] With regard to electronic documents, the new legislation follows the standard of giving full legal effect to electronic documents, but it does so "*provided that […] they are organized and stored in a way that preserves their safety*" and clarifies that "*[a]ny electronic writing that does not meet the criteria above shall be considered as introduction of written evidence*" (Article 4). While this condition, applied by many other countries in the region, appears to promote cybersecurity measures, it

[2] *See* (Dentons 2019)

unnecessarily limits the scope of the electronic documents. Under a strict reading, it would seem to suggest that documents such as email or non-encrypted documents may not be fully recognized as electronic documents equivalent to paper documents.

B. Electronic signature

The ability to conclude legally binding contracts remotely, without the face-to-face interaction of the parties, is a central feature of global business. Digital technologies reduce distances by facilitating interaction and collaboration across borders; electronic signature complements that digital proximity by providing a mechanism which grants full legal recognition to any agreement that may be concluded, even at a distance.

Digital activity involves engaging in remote—often international—contracts on a routine basis, to the point where users are not often aware of its international nature. For instance, accepting the terms of use of a website or a mobile app (often without even reading the content) by clicking a box entails, in legal terms, the acceptance of a contract through an electronic signature. For the developer of the app or the supplier of the online service, it is hence essential that the legal framework provide that such signature is indeed a recognized form of signature –in other terms, of accepting the terms of the contract.

Electronic signatures are particularly important to transactions between firms, especially in the context of a global or regional value chain. While e-commerce transactions by final consumers are typically individual purchases of discrete goods or services that can be satisfied with a simple click on a box, cross-border deals between firms often involve a business relationship that extends in time and entails the production and delivery of customized goods or services, whose terms and specifications need to be clearly agreed to in advance. This type of B2B interaction must be reflected on a distinct, specific, contract between the client and supplier, sanctioned with the signature of the parties to accept that those are the agreed terms. For these engagements, the parties may wish to back those digital documents with an electronic signature that provides certain guarantees against tampering or prying by third parties.

International guidelines and practice

At a minimum, a regulatory framework should recognize that electronic signatures are a legally valid form of accepting an obligation or terms of a document. Further, the framework should also ensure that, when an electronic signature meets certain requirements, it has full recognition of validity and enforceability, just like a handwritten signature.[3]

The UN Convention on the Use of Electronic Communications in International Contracts provides that e-signatures should satisfy a legal requirement for a signature so long as the e-signature meets certain requirements. The method used to identify the party's intention in respect of the information attached must be either as reliable as appropriate for the purpose of the electronic communication or proven to have fulfilled the requirements. The Convention's scope is limited to contracts between parties whose places of business are in different countries, and it

[3] Handwritten signatures, in addition to being legally valid, are also enforceable as they create the presumption that they were indeed inserted by the designated person (a *rebuttable* presumption, that allows the interested person to show proof, for instance, that the signature had been forged). Electronic signatures can be recognized as legally valid but may or may not be given full enforceability depending on the technology and procedures in use. Typically, only "digital signatures" that use some type of encryption technology are given full enforceability –*see* Box 1 for further details. An electronic signature that is not fully enforceable would require that the person claiming its validity also provide evidence that such electronic signature was indeed inserted by the designated person.

excludes certain transactions, including contracts for family or household purposes and transactions on a regulated exchange.

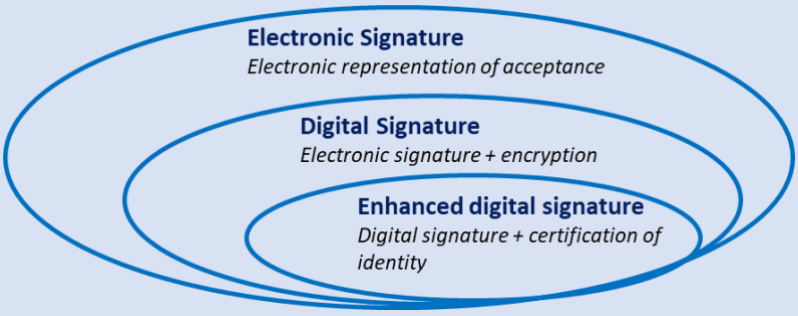
UNCITRAL Model Law on Electronic Signatures (MLES) of 2001 provides the standards required for an e-signature to be considered legally equivalent to handwritten signatures. It also lays out basic rules of conduct regarding the responsibilities and liabilities of the parties, including the signatory, the certification service provider (CSP), and the relying party. Any method of creating an electronic signature satisfies a legal requirement for a signature.

When certain conditions are met, regulation may extend to electronic or, more often, digital signature, the same treatment that it affords to handwritten signatures: that the signature is not only legally valid, but also that it belongs to the signatory (authenticity), and that the signature itself and the information to which is relate has not been altered (integrity). If deemed sufficiently reliable, foreign certificates and electronic signatures are recognized regardless of the place of issuance of the certificate, creation or use of the signature, or place of business of the issuer or signatory.

Box 1: Electronic Signatures vs. Digital Signatures vs Enhanced Digital Signatures

Although the terms electronic signature and digital signature are sometimes used interchangeably, a digital signature is actually a type of electronic signature. An electronic signature is defined by Oxford Dictionary as "symbols or other data in digital form attached to an electronically transmitted document as verification of the sender's intent to sign the document". In practice, an electronic signature is an electronic representation that the person has agreed to the content of the document, be that in the form of a typed name ("*John Lennon*"), an image of the person's handwritten signature (), or any other form electronic representation, such as an image () or icon () or simply the clicking of a box with a ✓.

Digital signature is defined as "a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate". Whereas an electronic signature can be created by simply clicking a mouse or tracing a handwritten signature with a finger, digital signatures involve the use of a code or algorithm to sign and validate the authenticity of a document. Unlike electronic signatures, digital signatures come under specific standards and a stringent verification process. A digital signature ensures the integrity of a message. This is achieved through a series of steps. First, the receiver's public key is used to encrypt a random key. This is combined with the encrypted message as well as the digital signature and the authenticated message is transmitted through an unsecured network. Upon receipt, the message is separated from the digital signature and the receiver's private key is used to decrypt it. A temporary digital fingerprint, hashed from the random key, validates the received fingerprint. If the message has not been corrupted during transmission, it is authenticated.



Digital signatures are most commonly created through a technology known as "Public Key Infrastructure" (PKI), which provides a cryptographic key pair that can be shared through a trusted authority. The use of the keys not only encrypts the message so that only the intended recipient can access it, but it also guarantees that the content of the message has not been violated or altered.

The mere use of PKI, however, cannot guarantee that the person who sent the message is indeed the person who he/she claims to be. Indeed, one person could be sending secured messages using an alias. To prevent this, an "enhanced digital signature" (or "secure digital signature" in some countries) is a digital signature that belongs to a person whose identity has been verified by a relevant authority. An enhanced digital signature

typically involves, in addition the use of a PKI : i) a certificate service provider (CSP)—typically an IT firm who offers electronic signature technologies, such as DocuSign or Adobe, and has been vetted to issue such certificate— who generates, stores, issues, renews, revokes, and verifies the digital certificates, and ii) a registration authority who verifies the identity of entities before their digital certificates are stored at the CSP, which could be a public entity or a private one, depending on the regulation.

With the growth of e-commerce around the world, governments have enacted legal instruments to give recognition and legal validity to electronic and digital signatures. While the objective of all these regulations is recognizing some kind of electronic representation as a legally valid signature, three different regulatory models are currently in place ((Frederick Fischer 2001); (Blythe 2011)).

- On one end of the spectrum, the **prescriptive approach** only recognizes one type of e-signature as legally valid –typically, digital signatures that have adopted specific encryption mechanism and have been issued following prescribed procedures. While secure digital signatures have the advantage of offering the maximum degree of security, the prescribed technology and procedures is unnecessarily costly and burdensome for most activities, as the parties may be forced to resort to certification authorities and pay a fee thereto. This approach was pioneered in the state of Utah, and later replicated in other states in the United States and countries around the world, including Bangladesh, Brazil, and Peru ((Blythe 2011); (Adobe 2019)).
- A "minimalist" or **"permissive" approach**, on the contrary, allows parties to choose the technology they prefer, giving any selected technology equal legal validity. The United States, Canada, Australia, and New Zealand have adopted this approached (AssureSign 2019). This approach affords the greatest liberty to the parties in adopting any type of technologies, thus reducing costs. However, the approach fails to acknowledge that certain technologies are indeed more secure than others and the greater security may be warranted in certain conditions.
- A hybrid or **"two-tiered" approach** is a mix between these two, recognizing all technologies as legally valid while giving certain presumptions (authenticity, integrity, etc.) only to digital signatures. Like the prescriptive approach, it describes the requirements of a digital signature, and includes rules of conduct regarding the rights and responsibilities of the parties, including the signatory, the certification service provider (CSP), and the relying party. A few countries have further developed this approach to offer greater liberty to private parties in adopting digital signatures through technologies of their own preference or allowing certification by non-accredited CSPs.

Singapore has further elaborated the two-tiered model creating a third category of signature. With a view to increasing security while reducing costs of adoption, Singapore's Electronic Transactions Act allows private parties to adopt any *commercially reasonable security* available that, to the extent that it could provide equivalent security as the prescribed mechanism for digital signatures, they would also be granted the same treatment as handwritten signatures. This model essentially extends flexibility to the parties in selecting a technology and a certification provider of their choosing. Other countries, like Mexico and Colombia, have followed this model in their more recent regulations. The EU Electronic Identification and Authentication Services Regulation (eIDAS) of 2016 also opened the door for EU Members to recognize an

"advanced digital signature" that has greater flexibility in the type of encryption technology and selection of CSP.

The hybrid approach has become the preferred method of regulating electronic signatures around the world. In 1998, Singapore introduced the first law of this type, later amending it in 2010 to bring it in line with the UN Convention, and it has become the trend in modern electronic signature regulation, having been adopted by the European Union; China; Hong Kong SAR, China; Japan; and the Republic of Korea, among many others (Blythe 2011). This approach is preferable as it sets out the use of a specific technology (PKI) and procedures (certification services providers) to ensure that secure digital signatures can indeed guarantee the identity of the signatory and integrity of the content. These specific procedures are required, for instance, for submitting documents to the government.

Most countries in the sample have adopted the hybrid approach, recognizing all e-signatures as legally valid while giving greater evidential weight to digital signatures (Table 3). While some of these regulations grant specific legal presumptions to secure digital signatures, such as integrity or intent, others are broader, granting them the presumption of reliability. Some countries followed Singapore's example, extending the legal presumptions to all digital signatures meeting certain criteria, regardless of the certification service provider or technology used. Countries in Central Asia –such as Armenia, Kazakhstan, and Moldova— maintain the prescriptive model, which is unduly

Table 3: Regulations on electronic signature around the world

	Model adopted	Flexibility in CSP or technology used	Certification authorities
Albania	Two-tiered	Yes	National Authority for Electronic Certification
Armenia	Prescriptive	Yes	"Authorized Body"
Bangladesh	Prescriptive	Yes	Controller of Certifying Authority
Burkina Faso	Two-tiered	No	Regulatory Authority of Electronic Communications
Canada	Permissive	Yes	Treasury Board
Colombia	Two-tiered	Yes	Superintendence of Industry and Commerce
France	Two-tiered	No	National Agency for Information Systems Security
Honduras	Two-tiered	Yes	Directorate General of Intellectual Property
Indonesia	Prescriptive	Yes	Minister of Communications and Informatics
Kazakhstan	Two-tiered	No	National Certification Authority
Kenya	Prescriptive	Yes	Communications Commission
Korea, Rep.	Two-tiered	No	Korea Information Certificate Authority
Kyrgyzstan	Two-tiered	No	State Committee of Information Technologies and Communications
Malaysia	Two-tiered	No	Controller of Certification Authorities
Mexico	Two-tiered	Yes	Secretariat of Economy
Moldova	Two-tiered	No	Information and Security Service
Pakistan	Two-tiered	Yes	Electronic Certification Accreditation Council
Senegal	Two-tiered	Yes	State Information Technology Agency
Tanzania	Two-tiered	No	Communications Regulatory Authority
Vietnam	Two-tiered	No	Root Certification Authority

restrictive as it requires the use of specific technologies, such as encryption, to recognize the validity of the e-signature. All countries in the review allow commercial firms to provide legally recognized certifications, and some, such as Armenia and Kyrgyzstan, allow for certification by non-authorized CSPs. Providing these options reduces the costs of adoption as parties to a transaction have alternatives to choose from when seeking certification.

MENA

Most of the countries in the MENA region have adopted regulation that recognizes electronic signatures as legally valid, adopting a two-tiered model (Table 4). In the majority of the countries, parties to a contract may choose any method of signing that they deem appropriate given the circumstances. However, in most cases, the use of a digital signature with a certificate issued by a certification service provider licensed by the authority is given evidentiary presumptions, including the presumption of validity and authenticity. Other countries in the region have implemented the prescriptive approach, only viewing digital signatures as legally valid, regardless of the circumstances. This can be restrictive, as it does not allow the parties to a contract to select the technology that best suits their needs.

Table 4: Regulations on electronic signature in MENA

	Model adopted	Flexibility in CSP or technology used	Certification authorities
Algeria	Two-tiered	No	Economic Authority of Electronic Certification
Bahrain	Two-tiered	No	No accredited CSPs to date
Djibouti	None	N/A	N/A
Egypt, Arab Rep.	Prescriptive	N/A	ITIDA operates the Egyptian Root Certificate Authority and issues licenses for CSPs.
Iran, Islamic Rep.	Two-tiered	Yes	N/A
Iraq	Two-tiered	No	N/A
Israel	Two-tiered	Yes	Registrar of Certification Authorities
Jordan	Two-tiered	Yes	N/A
Kuwait	Two-tiered	No	N/A
Lebanon	Two-tiered	No	Lebanese Accreditation Council (COLIBAC).
Morocco	Two-tiered	No	Directorate General of Information Systems Security
Oman	Two-tiered	Yes	Information Technology Authority
Qatar	Two-tiered	No	National Center for Information Security
Saudi Arabia	Two-tiered	Yes	National Center for Digital Certification
Tunisia	Prescriptive	N/A	National Agency for Digital Certification
United Arab Emirates	Two-tiered	Yes	Controller
Yemen, Rep.	None	N/A	N/A

Some MENA countries still feature burdensome models, and implementation is uncertain across the region. The Arab Republic of Egypt and Tunisia maintain prescriptive models that unnecessarily limit the options of private parties to choose a type of e-signature appropriate for their circumstances.

While other countries have adopted seemingly more liberal regulation, implementation remains uncertain across the region. For instance, Bahrain has to date accredited no certification services

providers.[4] This means that no firm or individual can adopt a secure digital signature, thus severely crippling the framework for e-signatures. Information regarding the certification authorities of other countries in the region, including Jordan and Kuwait, is also not available online, reducing the effectiveness of the system in the best-case scenario. All other countries have appointed public entities as certification authorities, which often leads to poor implementation when the agencies are not adequately trained and equipped. However, all MENA countries allow for certification by private certification providers, which can help mainstream the use of digital signatures.

III. Trust-building regulation

Regulation plays an essential role in bolstering digital markets by promoting trust. As digital markets are still in their infancy, the top reason for not engaging in online purchases, at least in developed markets, remains the lack of trust in remote electronic transactions (Figure 2). Consumers typically have no face-to-face contact with vendors, which leads to few "visual cues", such as location, facilities, and personalized interaction, which helps consumers gauge the retailer or suppliers' professionalism. In this environment, consumers are asked to disclose sensitive information and personal data either to a retailer, online intermediary, or digital platform. As a result, one important limiting factor in both developed and developing economies is the perception that cross-border online transactions and delivery are less secure, and remedies do not exist for when something goes wrong (World Economic Forum 2019).

Three sets of regulations are particularly relevant to promoting consumers' trust in digital markets:

- An effective framework for *online consumer protection* helps consumers be better informed about the characteristics of the good or services at hand as well as the terms of the transaction, promoting a greater understanding of the conditions of the transaction;
- As consumers are required to provide sensitive personal and financial details, a strong *data governance* regime is essential to give individuals control over their own information;
- Similarly, a *cybersecurity* framework further improves trust by ensuring that firms meet certain minimum technical standards in the protection of their digital information and that illegal access to such data is duly prosecuted and, if needed, penalized.

Figure 2. Lack of trust is the top reason for not purchasing goods and services online

[4] (International Trade Administration 2019)

Source: (CIGI-Ipsos 2017)

Trust-building regulation for digital markets is underdeveloped in MENA countries. Most countries in the region have not adopted frameworks specific to online consumer protection, data governance, and cybersecurity, by rather relying on general frameworks that were not designed for digital transactions. Even those who advanced on specific provisions for online transactions, such as Algeria, Qatar, and Tunisia, are missing important elements of the regulation.

A. Online consumer protection

Online consumer protection is essential to support a global market for digital goods and services. Distance shopping presents challenges, such as the inability to assess products in person before confirming a transaction. Online consumer protection laws aim to ensure "a level of protection not less than that afforded in offline commerce" (UNCTAD, Consumer Protection in Electronic Commerce: A Note by the UNCTAD Secretariat 2017) (Bartley Johns, et al. 2017). To that end, *online* consumer protection builds on the principles and mechanisms of traditional consumer protection regimes, extending and adapting those protections to digital markets, in order to reduce some of the challenges of buying and selling online, such as the rights and obligations involving an electronic transaction, or the way to rescind it if necessary (OECD, Guidelines for Consumer Protection in the Context of Electronic Commerce 2000).

A detailed framework for online consumer protection should include digital-specific protections at all stages of the transaction. Consumer concerns include the conditions for the sale (pre-purchase), whether the goods purchased online will meet their expectations when they arrive (purchase), and whether they are entitled to any remedies if any problems arise during or after the transaction (post-purchase). These can be addressed through regulations addressing information disclosure requirements, the right to withdraw from a transaction, dispute resolution, and redress (Figure 3).

Figure 3. Stages of consumer protection regulations

International guidelines and practice

According to UNCTAD's Global Cyberlaw Tracker, only about 50 percent of countries around the world have some degree of protection for online consumers. Traditional consumer protection

laws have existed long before the emergence of the internet, and the protections can also extend, at least partially, to online transactions. However, shopping on the internet brings new legal challenges, and while some have introduced new legislation or updated consumer codes to include specific provisions for electronic transactions, most countries still lack a comprehensive regime for online consumer protection.

One particular consideration is whether to establish specific regimes tailored to transactions through e-commerce platforms. Solutions on this area differ widely. For instance, China places extensive responsibilities on e-commerce platforms to the extent that platforms will be held liable if they fail to provide information on offending vendors, whereas the United States and the European Union place more responsibility on users (World Economic Forum 2019).

The key principles for online consumer protection are recognized in two main international soft-law instruments. In 2016, the Organization for Economic Co-operation and Development (OECD) revised its Recommendation on Consumer Protection for E-commerce of 1998, modernizing its approach to fair business practices, information disclosures, payment protections, unsafe products, dispute resolution, enforcement and education. Similarly, the UNCTAD Guidelines on Consumer Protection of 1985 (revised in 1999) were updated in 2015 to include recommendations directed to protecting online consumers and improving transparency in online transactions. The Guidelines also recommend cooperation among countries, including in terms of information exchange and enforcement activities.

Box 2: General Principles for Consumer Protection for E-commerce from OECD Recommendation

Pre - Purchase

1. Transparent and effective protection: consumers who participate in e-commerce should be afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce.
2. Fair business, advertising and marketing practices: businesses engaged in e-commerce should pay due regard to the interests of consumers and act in accordance with fair business, advertising and marketing practices as well as the general principle of good faith.
3. Online disclosures: online disclosures should be clear, accurate, easily accessible and conspicuous so that consumers have sufficient information to make an informed decision regarding a transaction. Online disclosures comprise the following areas of recommendations:
    a. Information about the business: businesses engaged in e-commerce with consumers should make readily available information about themselves that is sufficient to allow, at a minimum: i) identification of the business; ii) prompt, easy and effective consumer communication with the business; iii) appropriate and effective resolution of any disputes that may arise; iv) service of legal process in domestic and cross-border disputes; and v) location of the business.
    b. Information about the goods and services: businesses engaged in e-commerce with consumers should provide information describing the goods or services offered that is sufficient to enable consumers to make informed decisions regarding a transaction.
    c. Information about transaction: businesses engaged in e-commerce should provide information about the terms, conditions, and costs associated with a transaction that is sufficient to enable consumers to make an informed decision regarding a transaction. Consumers should be able to easily access this information at any stage of the transaction.

Purchase

4. Confirmation process: businesses should ensure that the point at which consumers are asked to confirm a transaction, after which time payment is due or they are otherwise contractually bound, is clear and unambiguous, as should the steps needed to complete the transaction, especially for new payment mechanisms.

Post - Purchase

5. Dispute resolution and redress: consumers should be provided with meaningful access to fair, easy-to-use, transparent and effective mechanisms to resolve domestic and cross-border e-commerce disputes in a timely manner and obtain redress, as appropriate, without incurring unnecessary cost or burden. These should include out of court mechanisms, such as internal complaints handling and alternative dispute resolution. Subject to applicable laws, the use of such out-of-court mechanisms should not prevent consumers from pursuing other forms of dispute resolution and redress. (See below sub-section on online dispute resolution and redress.)

6. Privacy and security: businesses should protect consumer privacy by ensuring that their practices relating to the collection and use of consumer data are lawful, transparent and fair, enable consumer participation and choice, and provide reasonable security safeguards (see section on data privacy).

Other

7. Education, awareness, and digital competence: governments and stakeholders should work together to educate consumers, government officials, and businesses about e-commerce to foster informed decision making. They should work towards increasing business and consumer awareness of the consumer protection framework that applies to their online activities, including their respective rights and obligations, at domestic and cross-border levels.

Source: **(OECD, Guidelines for Consumer Protection in the Context of Electronic Commerce 2000)**

Table 5. Regulation on online consumer protection around the world

	Online consumer protection regulation		
	None	General	Specific
Albania		•	
Armenia	•		
Bangladesh	•		
Burkina Faso			•
Canada*			•
Colombia		•	
France			•
Honduras		•	
Indonesia		•	
Kazakhstan		•	
Kenya		•	
Korea, Rep.			•
Kyrgyzstan		•	
Malaysia			•
Mexico		•	
Moldova			•
Pakistan*		•	
Senegal			•
Tanzania			•

Vietnam			•

(*) Template approved by federal, provincial and territorial ministers responsible for consumer affairs
(**) Consumer protection is a provincial subject, regulated in Karachi through the Sindh Consumer Protection Act

Of the domestic regulations analyzed, most have introduced online consumer protection provisions. Some of these protections can be found in e-commerce specific laws or in provisions under a general consumer protection law (Table 5). Laws specific to e-commerce offer the opportunity to fine tune the regulation to online transactions, and hence provide for a more comprehensive and tailored regulation that is not guaranteed by the mere enacting of a consumer protection law.

All the countries found to have online consumer protection regulations require that online sellers disclose certain information before the terms of the contract are accepted (Table 6). Some countries, such as Honduras and Kazakhstan, take this a step further, requiring the online disclosures be provided in the country's official language. While Kenya requires the disclosure of "prescribed information", the government has not specified what this information is.

Most of these countries follow OECD recommendation to provide online consumers a period of time to cancel a contract after purchasing a product or service online. The EU Directive on Consumer Rights grants online consumers the right to withdraw from distance contracts within fourteen days (Article 9). Consumers may withdraw from a contract if they do not like the product or they changed their mind. The consumer bears the direct cost of returning the goods, unless the trader agreed to bear it or failed to inform the consumer of the responsibility (Article 14, para. 1). On the other hand, Kenya's Consumer Protection Act gives online consumers seven days to cancel a contract, provided that (1) the seller did not provide certain online disclosures, or (2) the seller did not allow the consumer to accept or decline the contract or to correct mistakes prior to concluding the transaction (Article 33). Canada's Internet Sales Contract Harmonization Template has similar conditions for the cancellation of an online transaction.

France and Mexico stand out with regard to dispute resolution, providing online mechanisms to resolve disputes for e-commerce transactions. The European Commission's Online Dispute Resolution platform allows online consumers to lodge complaints in any EU language, in addition to Icelandic, and Norwegian. Consumers may use the platform to communicate directly with the seller regarding their claim, or they may choose to go through a mediator on the platform. The European Commission posts an online list of approved mediators for the consumers' convenience. Mexico has followed a similar approach, providing an option to resolve disputes online. According to Mexico's Consumer Protection Law, dispute resolution may be carried out via telephone or any appropriate means. The Office for the Federal Prosecutor for the Consumer allows online consumers to submit complaints via Concilianet, an online dispute resolution platform. Following the online conciliation hearing, users are able to may review the service provided by the platform. On the other hand, while their regulatory frameworks do not provide for online dispute resolution, Canada, Colombia, Korea, and Vietnam are members of e-consumer.gov,[5] a partnership of 36 consumer protection agencies worldwide that provides, among other services, an international platform to address cases of cross-border claims.

[5] e-consumer.gov is a web-based service developed by the International Consumer Protection and Enforcement Network (ICPEN). ICPEN is a network of governmental organizations in the enforcement of fair-trade practice laws and other consumer protection activities. E-consumer.gov is one of the first examples of an international ODR

Table 6. Domestic regulations on online consumer protection

	Pre-Purchase				Post-Purchase				
	Information disclosure requirements (*)				Withdrawal		Dispute Resolution	Options for redress	
	a.	b.	c.	d.	Existence of right	Absence of Reason	Online mechanism	Refund	Other options
Albania	•	•	•	•	•	•		•	•
Armenia									
Bangladesh									
Burkina Faso	•	•	•	•	•	•		•	
Canada	•	•	•					•	
Colombia	•	•	•	•	•	•		•	•
France	•	•	•	•	•	•	•	•	•
Honduras	•	•	•		•	•		•	•
Indonesia	•	•	•					•	•
Kazakhstan	•		•		•	•		•	•
Kenya					•			•	
Korea, Rep.	•	•	•	•	•			•	
Kyrgyzstan	•	•	•		•	•		•	•
Malaysia	•	•	•					•	•
Mexico	•	•	•	•	•	•	•	•	•
Moldova	•	•	•		•			•	•
Pakistan	•		•					•	•
Senegal	•	•	•	•	•	•		•	•
Tanzania	•	•	•		•	•			
Vietnam	•	•	•	•				•	•

(*) Information on a. merchant's address; b. payment process and/or delivery conditions; c. product specifications; d. complaint handling

Most regulations allow online consumers to obtain redress for harm suffered as a consequence of goods or services that are defective or do not meet advertised quality criteria. This usually takes the form of a monetary remedy (e.g. refund or price reduction) or a conduct remedy with a restorative element (e.g. exchange or repair). While Burkina Faso, Canada, Kenya, and Korea only offer refund as an option for redress, the rest of the countries provide alternatives to refunds.

MENA

Table 7. Adoption of regulation on online consumer protection in MENA

	Online consumer protection regulation		
	None	General	Specific
Algeria			•
Bahrain		•	
Djibouti	•		
Egypt, Arab Rep.		•	
Iran, Islamic Rep.			•

platform, meant to help consumers and agencies to combat international scams. It allows consumers to make cross-border fraud complaints in several languages (English, French, German, Korean Japanese, Polish, Spanish, and Turkish) and across many industries (e-commerce, banking, tourism, lottery, etc.). It is also a secured platform hosted by the U.S. Federal Trade Commission for law enforcement to share and access consumer complaints.

Iraq	•		
Israel	•		
Jordan	•		
Kuwait	•		
Lebanon		•	
Morocco		•	
Oman	•		
Qatar			•
Saudi Arabia			•
Tunisia			•
United Arab Emirates	•		
Yemen, Rep.	•		

Online consumer protections are scarce in the MENA region. Only about a handful of MENA countries have introduced legislation to address consumer protection for online transactions, most of these found in regulations specific to e-commerce (Table 7).[6] In the case of the regulations enacted in Bahrain, Qatar, and Saudi Arabia, while they are a step in recognizing the specific features of digital transactions, they fall short from offering a comprehensive regime and leave much room for further development.

Regulations on pre-purchase information are the most common in MENA online consumer protection regimes. All MENA countries with online consumer protection regulation require the essential information disclosures on product specific and transaction conditions. Regulations on post-purchase, even for countries that have enacted specific laws for e-commerce, remain limited. Of the countries that provide for the right of withdrawal, none requires a reason to exercise this right, and they allow a cooling-off period of between three and ten days. Options for consumer redress in the case of defective or inadequate products purchased online vary throughout the region, with refund being the most common tool provided to online consumers (Table 8).

Lebanon stands out in the region, addressing pre-purchase as well as post-purchase issues in its consumer protection law, which covers electronic transactions. Lebanon is the only country in the region that has set out a procedure for dispute settlement for e-commerce, providing that disputes up to 3 million Lebanese pounds (about US$2,000) for online transactions are subject to mediation.

Table 8. Regulations on online consumer protection in MENA

	Pre-Purchase				Post-Purchase				
	Information disclosure requirements (*)				Withdrawal		Dispute Resolution	Options for redress	
	a.	b.	c.	d.	Existence of right	Absence of Reason	Online mechanism	Refund	Other options
Algeria	•	•	•	•				•	•
Bahrain	•		•					•	•
Egypt, Arab Rep.	•	•	•		•	•		•	•
Iran, Islamic Rep.	•	•	•		•	•		•	
Lebanon	•	•	•	•	•	•		•	•
Morocco	•	•	•		•	•		•	•
Qatar	•	•	•					•	•
Saudi Arabia	•	•	•		•	•			
Tunisia	•	•	•		•	•		•	

(*) Information on a. merchant's address; b. payment process and/or delivery conditions; c. product specifications; d. complaint handling

Although none of the MENA regulations provides for an online dispute resolution mechanism, Egypt, Israel, Qatar, Saudi Arabia, and UAE are e-consumer.gov members. This solution,

[6] Secondary sources refer to online consumer provisions present in Israel's consumer protection regulations, but these regulations have not been found online

together with a consumer protection laws present in Egypt, Qatar, and Saudi Arabia that explicitly apply to digital transactions and expand consumers rights, creates some of the stronger frameworks for online consumer protections in the region.

B. Data governance

Consumers are increasingly aware of the value of their personal data. Lack of trust in the way personal data is managed drives consumers away from electronic transactions, limiting the growth of digital markets. At the same time, burdensome regulations on the use and transfer of individual data can build substantial costs for businesses, especially small and medium enterprises. The goal is hence to allow data transfers in a manner that supports the expansion of digital markets, while increasing consumer trust that their private information remains secure and under their control.

Data governance legal frameworks consist of entitling rights for all or certain types of individuals (also called data subjects) regarding the collection, usage, storage, and disposal of their personal data. They also create obligations for controllers and processors while enacting derogations in certain circumstances (state security, public safety, etc.). Security processes for data controllers (either public or private) ensure the appropriate processing of personal data.

International guidelines and practice

Countries have unequally embraced data governance legal frameworks. The 1970s and 1980s saw a surge in personal data protection regulation, with several European countries enacting laws and several international organizations, such as the OECD, enacting instruments addressing the issue. But at the time, regulation arose for large government-owned data sets. Since the 1990s, digital communications led to the collection of massive data from private companies, which led to a new generation of legal frameworks to strengthen personal data protection and consumers' trust. However, while some countries have strived to modernize their privacy frameworks to reflect the challenges of the new digital technologies, many countries lag and still rely on broad privacy principles set out in the constitution or elaborated in older privacy laws.

Europe has been at the forefront of the most comprehensive (and costly) legislation on data protection. It had a significant impact on other countries' legislation (see below). The United States developed a less stringent and comprehensive framework which mostly relies on industry-related best practices. Canada and Latin American countries developed privacy frameworks in the 1990s and 2000s partly in the form of habeas data. Asia and Oceania have seen their most developed countries adopting data governance laws (Australia; New Zealand; Hong Kong SAR, China; Korea) while others remain lagging. The Middle East and Africa have the least developed data governance legal frameworks.

Several international instruments have been focused on setting out the key principles of data governance regulation. Most recently, the Digital Economy Partnership Agreement (DEPA) between Singapore, Chile, and New Zealand recognized the need for international collaboration on matters relating to the digital economy, including data governance. The Asia-Pacific Economic Cooperation (APEC) Privacy Framework of 2015 promotes a flexible approach to privacy protection, with a focus on avoiding the creation of unnecessary barriers to information flows. The Convention "108+" by the Council of Europe is an international human rights treaty focused on data protection, setting out principles that are compatible with the requirements of the European regulation. In 2013, OECD members updated their Guidelines on the Protection of

Privacy adopted in 1980 to account for the new reality of digital data flows. The OECD Guidelines declare digital risk an economic risk and they aim to protect privacy and individual liberties with respect to personal data process in the public or private sector. They include eight basic principles for data protection:

- **Collection limitation principle**: limits the collection of personal data and suggests lawful and fair means for collection, as well as consent of the data subject where appropriate
- **Data quality principle**: calls for relevancy of the personal data to the purposes for which they are to be used. Additionally, it calls for data accuracy, completion, and maintenance
- **Purpose specification principle**: data controllers should specify the purpose for which the data are collected no later than at the time of data collection. Subsequent use of the data should be limited to those purposes and the data subject should be notified of any change of purpose
- **Use limitation principle**: limits the use of the data for purposes other than those specified, with the consent of the data subject or by the authority of law
- **Security safeguards principle**: calls for reasonable protection of the data from risks such as loss or unauthorized access, destruction, use, modification, or disclosure of the data
- **Openness principle**: suggests a general policy of openness regarding developments, practices, and policies with respect to personal data
- **Individual participation principle**: the data subject should have the right to request data from a data controller or a confirmation of whether the data controller has personal data relating to the individual. If the data controller has such data, it should be provided to the data subject within a reasonable time, in a reasonable manner and in a form that is readily intelligible to the data subject
- **Accountability principle**: the data controller should be held accountable for abiding with principles of the Guidelines.

Most countries in the sample have introduced a substantial regulatory framework for data governance (Table 9). Some of the governments that do not currently have a regulatory framework in place are discussing draft regulations to address this.[7] On the other hand, Honduras has implemented an interim protection, inserting a provision in its e-commerce law that subjects data messages to constitutional and legal provisions which guarantee the right to communication privacy and access to personal information.

Misuse or breach of sensitive data usually leads to greater consequences for the data subject. Sensitive data may include special categories of information, such as a person's political views, sexual orientation, or medical history. Most countries studied address this, providing special rules for the treatment of sensitive personal data during processing (Table 10). Canada, Indonesia, Kazakhstan, and Vietnam stand out in that they feature a general framework on data governance, but do not provide special rules for the treatment of sensitive data.

[7] *See* Kenya—The Data Protection Bill, 2018.

Common principles for processing of personal data include the need to have a legitimate reason for any processing activity, usually obtained through consent of the data subject. Alternatives to consent address contractual or legal obligations the firm may be subject to as well as the interests of the data subject or the public. The majority of the regulations analyzed feature elaborate frameworks in this regard. An array of legal bases for data collection and processing gives processors more freedom under certain circumstances. Additionally, all the regulations reviewed required that personal data be stored in a manner that allows for the data subject's exercise of the right to access the information and to request its correction or deletion if necessary. While most of these requirements are included in the general frameworks for data governance, Honduras and Kenya grant these rights through the Constitution, and the Access to Information Act, respectively.

Table 9. Adoption of domestic regulation on data governance

	None	Partial	Full*	Comments
Albania			•	
Armenia			•	
Bangladesh	•			
Burkina Faso			•	
Canada			•	
Colombia			•	
France			•	
Honduras		•		The Constitution grants right to access and deletion
Indonesia			•	
Kazakhstan			•	
Kenya		•		Access to Information Act grants right to access and deletion
Korea, Rep.			•	
Kyrgyzstan			•	
Malaysia			•	
Mexico			•	
Moldova			•	
Pakistan	•			
Senegal			•	
Tanzania	•			
Vietnam			•	

(*) Refers to a general framework on privacy and data protection. Despite the lack of a general framework, specific rules may be often found in sectoral regulations, in particular on financial, telecommunications and health sectors

Providing clear rules on cross-border data transfers increases transparency and the ease of compliance. Here too, Vietnam's legislation stands out as the only one failing to provide such rules. Additionally, where data is required to be stored domestically, such requirement should not prevent processors from transferring a copy of the data abroad. This grants governments greater ease of accessing the data of their citizens during legal disputes, while ensuring global data flows. Although data localization requirements may be present in other regulations, such as those addressing financial or health matters, none of the general data governance frameworks analyzed feature this type of restriction.

Table 10: Domestic regulation on data governance around the world

	Sensitive data	Legal bases for data collection and processing				Data subject's rights	Cross-border data transfers	
	Special treatment	Consent	Performance of a contract	Legal obligation	Legitimate interests	Access/ deletion	Rules on transfers	No data localization
Albania	•	•	•	•	•	•	•	•
Armenia	•	•	•	•		•	•	•
Burkina Faso	•	•	•	•		•	•	•
Canada		•	•	•	•	•	•	•

Colombia	•	•		•		•	•	•
France	•	•	•	•	•	•	•	•
Honduras						•		
Indonesia		•		•		•	•	•
Kazakhstan		•		•		•	•	•
Kenya								
Korea, Rep.	•	•	•	•	•	•	•	•
Kyrgyzstan	•	•			•	•	•	•
Malaysia	•	•	•	•		•	•	•
Mexico	•	•	•	•		•	•	•
Moldova	•	•	•	•	•	•	•	•
Senegal	•	•	•	•		•	•	•
Vietnam		•	•	•		•		•

MENA

Few countries in the MENA region have introduced a comprehensive legislation to protect data privacy (Table 11). Algeria, Bahrain, and Morocco, appear to have established the strongest frameworks for data protection, taking elements from the EU Data Protection Directive of 1995 and, in the case of Bahrain's new law, from EU GDPR. Israel's main legislation on privacy protection dates back to 1981, but it has been complemented with additional regulations, resulting in a modern and strong framework. In 2003 Israel become the first and the only country to date in the region to have been officially recognized by the European Union as providing an "adequate level of protection" for personal data (CipherCloud 2017).

Table 11. Adoption of regulation on data governance in MENA

	None	Partial	Full*	Comments
Algeria			•	
Bahrain			•	
Djibouti	•			
Egypt, Arab Rep.	•			
Iran, Islamic Rep.			•	
Iraq	•			
Israel			•	
Jordan	•			
Kuwait		•		Basic rules on privacy in Electronic Transactions Law
Lebanon		•		Basic rules on privacy in Electronic Transactions Law
Morocco			•	
Oman		•		Basic rules on privacy in Electronic Transactions Law
Qatar			•	
Saudi Arabia		•		Basic privacy rules in e-commerce law
Tunisia			•	
United Arab Emirates		•		Data protection regime applies to Dubai
Yemen, Rep.	•			

(*) Refers to a general framework on privacy and data protection. Despite the lack of a general framework, specific rules may be often found in sectoral regulations, in particular on financial, telecommunications and health sectors

While some countries have set out strong regulatory frameworks, most regulations remain patchy, weak, or outdated. Some countries have included basic principles of data privacy in the context of broader regulations on e-commerce, such as Lebanon and Oman, providing hence an embryonic framework for data governance. Saudi Arabia features specific provisions on data privacy in its e-commerce law of 2019. These partial

regimes typically only focus on the legal basis for data collection and some rights of data subjects but fail to offer a comprehensive framework that differentiates personal from non-personal data, provides rules on transfer of data, or sets out conditions for conservation or destruction of personal data. UAE does not have a framework for privacy protection, but Dubai has adopted a full-fletched framework under the context of the Dubai International Financial Centre (DIFC) Authority that applies to business conducted in the special economic zone -thus having a geographical limitation to the scope of the regulation. Despite not having a comprehensive framework on data governance, provisions on personal privacy can be found in other countries in the region dispersed in sectoral or other specific regulations. For instance, in Egypt, the criminal code imposes a punishment for the unlawful collection of images or recordings of individuals in private places, and the Banking Law requires confidentiality for information regarding clients and accounts (CipherCloud 2017). These discrete provisions can be essential in their own context but should ideally be integrated in a broader framework that balances the different priorities of data privacy protection.

Table 12: Regulation on data governance in MENA

	Sensitive data	Legal bases for data collection and processing				Data subject's rights	Cross-border data transfers	
	Special treatment	Consent	Performance of a contract	Legal obligation	Legitimate interests	Access/ deletion	Rules on transfers	No data localization
Algeria	•	•	•	•	•	•	•	•
Bahrain	•	•	•	•	•	•	•	•
Iran, Islamic Rep.	•	•				•		•
Israel	•	•				•	•	•
Kuwait		•				•		•
Lebanon	•					•		•
Morocco	•	•	•	•	•	•	•	•
Oman		•		•		•	•	•
Qatar	•	•		•	•	•		•
Saudi Arabia		•		•				•
Tunisia	•	•	•			•	•	•
United Arab Emirates		•					•	•

All the existing comprehensive regulatory frameworks for data governance in MENA feature most of the crucial provisions, including special treatment of sensitive data and data subjects' rights with regard to their personal data (Table 12). The Islamic Republic of Iran and Israel failed to introduce alternatives to consent as legal bases for data collection and processing. All these regulations, except for those introduced by the Islamic Republic of Iran and Qatar, feature clear rules on cross-border data transfers. As seen in the other countries studied, none of these regulations include data localization requirements but this does not mean that such requirements are absent from sector-specific regulations.

C. Cybersecurity

While less visible to the individual consumers, cybersecurity regulation is an essential component for promoting trust in digital markets. Cybersecurity refers to the measures that can be implemented to protect personal data from unauthorized access and corruption. Major data breaches, like that which Yahoo witnessed in 2013—affecting 3 billion user accounts— not only

compromise people's privacy but can have a chilling effect for digital markets as consumers realize how vulnerable their information is.

In 2015, the OECD declared digital risk an economic risk (OECD, Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity 2015). If personal data is not securely processed it is more prone to breaches. Data breaches can occur in different ways, including unintended disclosure, hacking, and malware (Privacy Rights Clearinghouse n.d.).

Adequate cybersecurity regulations render data controllers and data processors liable for data processing. A data controller makes decisions over the purposes and means of the data processing, while a data processor processes data on behalf of controllers. For example, if an e-commerce platform hires a firm to track consumer activity on the platform, the e-commerce platform is the controller with regard to the information collected, while the firm is the processor.

International guidelines and practice

Security requirements consist of organizational and technical measures as well human resources. These may include mandatory encryption of personal data, implementation of rigorous internal policies, or the appointment of a data manager. Assessment of the risk to a data subject's privacy helps determine the adequate safeguards that need to be implemented (OECD, Privacy Guidelines 2013). Countries without adequate data protection regulations risk being avoided by companies due to the lack of certainty about compliance and data handling (Trade 2015). Additionally, these countries are missing out on the benefits of the Internet, such as innovation and economic growth (Forum 2016).

Following two significant U.S. government hacks that affected over 22 million people (Washington Post n.d.), the Executive Office of the President's Office of Management and Budget (OMB) issued new cybersecurity requirements for federal agencies (OMB 2017). These include:

- Breach response team designation
- Risk assessment, risk mitigation, and breach notification
- Periodic internal data protection policy review
- Annual reporting of satisfaction of cybersecurity requirements; data breaches reported; breach response plan; identification of breach response team; and confirmation of breach response team's preparation exercises.

The EU General Data Protection Regulation (GDPR), which went into effect in 2018, also introduced updated provisions to protect the personal data and privacy of EU citizens, including cybersecurity requirements (Table 13).

Table 13: EU GDPR cybersecurity requirements

Security of processing	Controllers and processors must ensure a level of security appropriate to the risk through measures such as data pseudonymization and encryption
Breach notification	In case of a personal data breach, controllers must notify the supervisory authority within 72 hours of becoming aware of the breach. In cases where the breach is likely to result in a high risk to the individual rights, the controller must notify the data subject of the breach without undue delay

Impact assessment	Where data processing is likely to result in high risk to individual rights, the controller must conduct an impact assessment prior to processing, including the foreseen measures to address the risks
Designation of data protection officer	Controllers and processors must designate a data protection officer under certain circumstances, including if the bulk of the processing activities require regular and systematic monitoring of data subjects on a large scale, or if it consists of processing of sensitive data on a large scale

A key aspect of data protection is who monitors and enforces the implementation of the regulation. The establishment of a capable and effective implementing agency is central to ensuring adequate implementation of the regulation and to providing individuals with a policing entity to which resort in case of violations. When it comes to the enforcement of cybersecurity measures, a single central regulator tends to be the most adequate solution, providing oversight and complaints management (UNCTAD 2016). They can inform data subjects about their rights, supervise and assist data controllers with regard to compliance, and ensure the enforcement of data regulations. Data protection requirements also include registration with the authority and notification of data processing activities (UNCTAD 2016). Depending on the ease, cost, and recurrence of these requirements, they may impose a burden for businesses trying to enter a foreign market (UNCTAD 2016). The OECD revised its privacy guidelines in 2013, highlighting the importance of establishing privacy enforcement authorities (OECD 2013).

Most countries that have adopted a comprehensive framework on data protection have buttressed it with a data protection agency (DPA). Certain countries, such as France, have had a DPA since the 1970s, when large state-owned datasets were the main concern of the public. While most DPAs are independent agencies, some countries have embodied them with ministries or policy-making bodies (Makulilo 2016).

Table 14: Cybersecurity measures around the word

	Encryption	Internal policy	Data manager	Risk assessment	Breach notifications	Supervisory authority
Albania		•				•
Armenia	•	•			•	•
Bangladesh						
Burkina Faso		•				•
Canada		•	•		•	•
Colombia		•		•	•	•
France	•	•	•	•	•	•
Honduras						
Indonesia	•	•			•	
Kazakhstan		•				•
Kenya		•				
Korea, Rep.	•		•	•	•	•
Kyrgyzstan		•	•		•	•
Malaysia		•				•
Mexico		•		•	•	•
Moldova		•				•
Pakistan						
Senegal		•				•
Tanzania						
Vietnam		•		•	•	•

All of the countries found to have a comprehensive framework for data governance have included cybersecurity requirements in these regulations (Table 14). These include administrative and technical controls to protect against accidental loss or destruction or unauthorized access of the data. While most countries only require the adoption of an internal policy or the performance of internal controls, some countries have additional requirements. France and Korea feature the most inclusive requirements, calling for data encryption under certain circumstances to prevent unauthorized access to the data; appointment of a data manager; procedures to assess the threats and risks to personal information; and notification of the data subject and/or the authorities in case of a data breach.

Also, most countries that regulate data privacy governance have a supervisory authority that monitors data processing activities. Although Kyrgyzstan's Law on Personal Data makes reference to the "authorized body", such body is not currently identified. About half of the countries that have a supervisory body require certain administrative procedures to lawfully process personal data. Data processors in Colombia and Kyrgyzstan must register with the supervisory authority. In Moldova, Senegal, and Tunisia, controllers must notify the authority of their intent to process personal data. In Armenia, notification requirements only apply to sensitive data or by request of the authorized body.

MENA

The framework for cybersecurity in the region follows the same pattern of limited development as data governance (Table 15). Even for those countries that have adopted broader privacy regulations, provisions on cybersecurity tend to be vague, requiring data processors to implement measures to protect the data from unauthorized access or damage, without any clear specifications on the nature of the measures. Israel and Qatar are the only countries featuring a comprehensive framework on cybersecurity, imposing obligations on data processors to adopt internal data protection policies, conduct risks assessments,, notify data subjects and/or authorities of any data breaches, maintain sensitive data protected encrypted (Israel), and appoint a Data Manager responsible for data security in the firm (Qatar) (Table 14).

Table 15: Cybersecurity measures in MENA

	Encryption	Internal policy	Data manager	Risk assessment	Breach notifications	Supervisory authority
Algeria		•				•
Bahrain		•	•			•
Iran, Islamic Rep.						
Israel	•	•		•	•	•
Kuwait		•				
Lebanon		•				
Morocco		•				•
Oman						
Qatar		•	•	•	•	•
Saudi Arabia						
Tunisia		•				•
United Arab Emirates						

Of the MENA countries found to have general data governance framework, the Islamic Republic of Iran stands out as the only one with no cybersecurity requirements and no supervisory

authority in charge of enforcing data protection policies. MENA countries should consider adopting a framework for cybersecurity (ideally, in parallel to, and complementary of, a data governance framework) including specific regulations, such as data encryption requirements and risk assessment procedures.

D. Intermediary liability

The internet's unparalleled ability to connect billions of individuals worldwide has boosted business models based on intermediation between vendors and consumers. E-commerce platforms like Alibaba, eBay, and Mercado Libre are based on offering consumers products from thousands of different providers rather than their own stock. "Gig economy" apps offer services such as rides, lodging, or delivery of food or groceries from firms and individuals. Other services rely on content such as video (YouTube, Vimeo), opinions and reviews of products or services (Yelp, Google), or information (blogs) developed by thousands of users, most of whom remain relatively unknown to the final consumer. The relationship between the intermediary (websites and apps) and the firms or individuals offering their own products or services is hence essential to the functioning of those digital transactions.

Intermediary liability rules are the set of provisions that distribute the liability between intermediaries (website and apps) and actual vendors or content developers when things go wrong. In other terms, intermediary liability is the responsibility that falls upon online intermediaries, such as search engines, application platforms, social networks, and broadband companies, for third-party content featured in, or products and services offered through, their website or apps. Just like intermediation is not a novel business model, intermediary liability rules are not new a legal concept –most such rules can be traced back to Roman law. Intermediary liability rules can in fact be broader rules that apply to online intermediaries (Gasser and Schulz 2015). However, specific rules of digital intermediaries are more likely to adapt to the particular conditions of digital markets.

Rules on intermediary liability need to strike a balance between protecting consumer rights and supporting the expansion of digital markets, including through intermediary platforms. While the good, service, or content may be offered or developed by third parties, intermediary platforms benefit from it by building their businesses around it. Digital intermediaries manage the relationship with the costumer, and they are often the largest, more sophisticated actor involved in the transaction. As such, regulations can impose on intermediaries (jointly with the third party) liability for fake or faulty products or services, or for offensive or illegal content, transacted through or featured in their services. On the other hand, intermediaries often do not have full knowledge of everything that is being offered by producers and content developers, who have greater control over it.

For digital intermediaries, responsibility may arise mainly from two types of conduct: the offering for sale of counterfeited products or the publication of unlawful content, such as images or text, by their users. The offering of fake products would normally entail a violation of intellectual property rules (typically trademark protection). Unlawful content can instead run against intellectual property rules when the content is unduly featuring other people's work (a violation of copyright protection) by for instance reproducing music or video without the authors' permission, or it may violate criminal law provisions such as rules against libel, hate speech, or child pornography, the protection of individual privacy or classified information, or amount to lèse-majesté crimes.

Rules on intermediary liability in MENA are generally at odds with a conducive framework for digital markets. Most countries in the region lack a specific framework for *online* intermediary liability, which results in overly stringent requirements that add risks and costs for digital platforms. Those who do provide for such a framework usually do not cover infringements related to intellectual property –a key aspect for providers for content platforms (YouTube) or social media (Facebook) or smaller local social platforms, who depend on content uploaded by third parties and may find themselves liable for violations incurred by their users. Intermediary liability rules appear as the most underdeveloped segment of digital regulations in MENA, possibly adding high risks and costs for online platforms for e-commerce and content.

International guidelines and practice

Typically, rules on online intermediary liability have two components: one attributing responsibility to the intermediary and another reducing its liability by removing the violation ("safe harbor"). For example, an intermediary would be held liable if it had knowledge that the product being offered was fake but could be exonerated from responsibility if it took steps to remove the product from its listings upon obtaining knowledge of the violation. Rules on responsibility pivot between no responsibility, actual knowledge of the infringement (the intermediary knew the content was unlawful), duty of knowledge (the intermediary should have known that the content was unlawful), or absolute responsibility (the intermediary is responsible in all conditions). Safe harbor provisions typically involve notice and take down procedures, which require that upon receipt of a notice regarding infringing content, the intermediary search and remove all copies of the infringing content.

Rules on liability for digital intermediaries are nascent and still evolving, and a global trend on the topic remains elusive. Even within countries, views on the extent of liability that should be imposed on intermediaries varies greatly between the content industry and the internet industry. Much of this tension is seen in the Unites States, home to some of the largest internet firms as well as content developers, which has traditionally resulted in strong protections of digital intermediaries, as well as far-reaching disciplines on intellectual property (Holland, et al. 2014). Content industry representatives claim that the lack of intermediary responsibility leads to an increase in online piracy and decreased revenue for content industries, which has led the American Association of Publishers (AAP) to advocate for sanctions imposed on intermediaries for failing to ensure the protection of copyrighted material (USITC 2017). On the other hand, internet industry representatives argue that an increase in intermediary liability is likely to increase costs and limit intermediaries' ability to combat piracy (USITC 2017). The U.S. Digital Millennium Copyright Act (DMCA) creates a safe harbor for intermediaries under certain circumstances, including if they unknowingly display, transmit, or store infringing content. Section 230(c) of the Communications Decency Act shields intermediaries from liability for most third-party content. However, when it comes to copyright infringement, they must meet certain conditions, including a notice and takedown requirement.

The notice and take down model has been replicated around the world. In June 2017, Germany passed a law imposing fines of up to €50 million upon online intermediaries who do not remove illegal content within twenty-four hours of notice. The Russian Federation's Federal Law No. 187 provides intermediaries with safe harbor protections based on a legal test which determines whether they knew or should have known about infringing content. Content owners are not required to notify intermediaries about infringing content, and instead may go directly to the courts to request an injunction to block the content. Taking it a step further, the notice and stay

down model featured in the EU Directive on Copyright of 2019 compels intermediaries to prevent any future transmission of the infringing content. Notice and stay-down requirements seek to ensure that infringing content will not be posted again.

Seeking to protect online freedom of expression, an international coalition released the Manila Principles for Intermediary Liability (Box 3). The Principles provide governments with standards for censorship and takedown laws which respect the users' rights while promoting innovation.

Box 3. Intermediary liability guidelines

The Manila Principles for Intermediary Liability were developed to protect online freedom of expression and to provide governments with standards for censorship and takedown laws that respect the users' rights. The effort involved civil society groups from around the world, led by the Electronic Frontier Foundation (EFF, USA), the Centre for Internet and Society (CIS, India), Article 19 (UK), KICTANET (Kenya), Derechos Digitales (Chile), Asociación por los Derechos Civiles (ADC, Argentina) and Open Net (Republic of Korea).

The proposed principles are:

1. *Intermediaries should not be liable for third party content: intermediaries should be exempt from liability for third party content where they did not modify the content; they must not be required to routinely monitor content on their network or platform;*
2. *An order by a judicial authority must be required for content restriction: an order from an independent and impartial judicial authority must be required for content restriction;*
3. *Requests for restrictions of content must be clear, be unambiguous, and follow due process: where an intermediary receives a restriction request before a court order is issued, they need not evaluate the legality of the content; the request must include its legal basis; sanctions should be imposed for bad faith restriction requests;*
4. *Laws and content restrictions orders and practices must comply with necessity and proportionality tests: restrictions should be specific to the content at issue, if applicable, limited in geographical scope; and not extend beyond its duration;*
5. *Laws and content restriction policies and practices must respect due process: parties must be provided the right to be heard and to appeal against restriction orders;*
6. *Transparency and accountability must be built into laws and content restriction policies and practices: applicable rules and transparency reports must be published online in a timely manner.*

Source: (EFF 2015)

At the international level, some principles on intermediary liability were included in recent trade agreements. The recent Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States, Mexico, and Canada Agreement (USMCA) set limits to intermediary liability in their intellectual property and digital trade chapters, respectively. Intermediaries are not liable for copyright infringements "that they do not control, initiate, direct, and that take place through systems or networks controlled or operated by them or on their behalf". However, they must remove or disable access to copyright infringing content on their networks upon obtaining knowledge of its existence.

Intermediary liability rules relating to criminal or civil infringement laws are being modernized for the digital environment. The proliferation of fake news in recent years has led countries to seek to reduce the amount of misinformation that citizens can find online. However, this raises concerns about content filtering, freedom of speech, and media manipulation. Singapore, who has been often criticized for its heavy control of the media (Leung 2019), recently introduced the Protection from Online Falsehoods and Manipulation to hold social media sites liable for third-party content published on their platforms. Noncompliant platforms are subject to fines and imprisonment if they do not remove the "misinformation" or publish "corrections" next to it. Industry groups fear that this new type of law allows governments to decide what is true or false,

endangering the freedom of expression and speech. Following a terrorist attack in a mosque in New Zealand, which was streamed live on Facebook, Australia passed a bill requiring social media platforms to promptly remove abhorrent violent user content shared on their sites. The acts covered by the new law include murder, torture, rape, and kidnapping. Other countries around the world, including France and Germany, are also tackling these issues through legislation.

Table 16: Regulation on intermediary liability around the world

	Liability Status	Safe harbor provisions	IPR infringements covered	Notice and take down requirements
Albania	Partial	Lack of knowledge; content removal		•
Armenia	N/A			
Bangladesh	Partial	Lack of knowledge; content removal		
Burkina Faso	Partial	Lack of knowledge; content removal		•
Canada	Partial	Lack of knowledge	•	
Colombia	N/A			
France	Partial	Lack of knowledge; content removal	•	•
Honduras	N/A			
Indonesia	N/A			
Kazakhstan	N/A			
Kenya	Partial	Lack of knowledge		
Korea, Rep.	Partial	Content removal	•	•
Kyrgyzstan	N/A			
Malaysia	Partial	Lack of knowledge; content removal	•	•
Mexico	N/A			
Moldova	Partial	Lack of knowledge; content removal		•
Pakistan	Partial	Lack of knowledge		
Senegal	Partial	Lack of knowledge; content removal		•
Tanzania	Partial	Lack of knowledge; content removal	•	•
Vietnam	Strict			•

Most of the countries studied address intermediary liability and provide online platforms with safe harbor provisions where infringing content is posted by third parties (Table 16). The most common conditions to avoid liability are lack of knowledge of the infringing content and removing or disabling access to the infringing content expeditiously upon obtaining knowledge or becoming aware of a likelihood of liability. Intermediaries are usually deemed to become aware upon being notified of the infringement. No countries studied in Latin America have introduced legislation on the issue.

Notice of infringement can take different forms depending on the domestic regulation. In some countries, anyone may request the removal of infringing content. Tanzania's Cybercrimes Act allows anyone to notify the intermediary of content infringing their rights as well as the rights of others (Article 45). Other countries only give this right to copyright holders. In Korea, copyright holders may request the removal of infringing content after providing evidence of the infringement. (Copyright Act Article 103). Intermediaries are required to remove the content immediately and to notify the third party as well as the copyright holder. If the third party proves that the content is posted based on legitimate rights, the intermediary must notify the copyright holder of the request and of the scheduled date of resumption. The intermediary is required to designate an agent responsible for processing removal requests. Malaysia intermediaries must remove infringing content within forty-eight hours of obtaining notice from copyright holders

(Copyright Act Article 43H). Upon receipt of a counter notification from the third party, the intermediary must provide the copyright holder with a copy of the counternotification and with notice that access to the content will be restored in ten business days. The copyright holder may seek a court order to restrain the third party from engaging in any infringing activity relating to the content on the intermediaries' platform. Finally, Canada has implemented a "notice and notice" regime. There, if a copyright holder notifies the intermediary of infringement, the intermediary must forward the notice to the third party.

In other cases, the removal of infringing content may be enforced through a judicial order or notification by relevant entities. While Albania's Law on e-commerce explicitly excludes IPR infringements from its scope (Article 2), it provides that the court or competent authorities may compel the removal of unlawful activity by intermediaries (Article 19). In France, an administrative authority may notify the intermediary of content infringing laws against terrorism and child pornography, giving the intermediary twenty-four hours to remove the content. Senegal's law on electronic transactions also took steps to prevent infringement related to terrorism or child pornography: platforms must provide a method for anyone to notify them of infringing content, and the platforms must inform the relevant authority of this content (Article 3).

MENA

Legislation throughout the MENA region focuses on content posted online, holding intermediaries liable for third-party content. Some countries have introduced safe harbor provisions, shielding intermediaries from liability if they lack knowledge of the infringing content or act expeditiously to remove it upon becoming aware of it (Table 17). All those regulations include notice and take down requirements, ensuring that the infringing content is not posted again.

Table 17: Regulation on intermediary liability in MENA

	Liability Status	Safe harbor provisions	IPR infringements covered	Notice and take down requirements
Algeria	N/A			
Bahrain	Partial	Lack of knowledge; content removal	•	•
Djibouti	N/A			
Egypt, Arab Rep.	Strict	N/A		•
Iran, Islamic Rep.	Strict	N/A		
Iraq	N/A			
Israel	N/A			
Jordan	N/A			
Kuwait	N/A			
Lebanon	Partial	Lack of knowledge; content removal		•
Morocco	Partial	Lack of knowledge; content removal	•	•
Oman	Partial	Lack of knowledge; content removal		•
Qatar	Partial	Lack of knowledge; content removal	•	•
Saudi Arabia	Partial	Lack of knowledge; content removal	•	•
Tunisia	Strict	N/A	•	•
United Arab Emirates	Strict	N/A		
Yemen, Rep.	N/A			

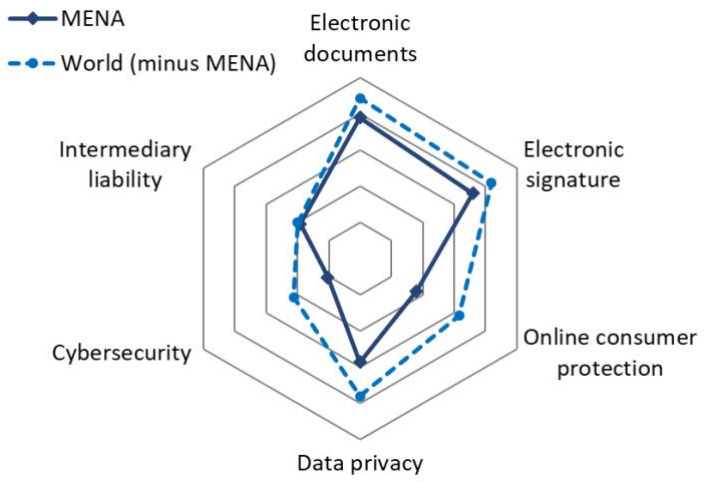
Most of the existing MENA regulations on intermediary liability appear aimed to govern situations involving criminal or civil sanctions, such as content that violates individual privacy, religious values, public morals, or national security. Intermediary liability rules in MENA do not seem to be directly linked to violations of intellectual property. Only Bahrain, Morocco, Qatar, and Saudi Arabia's regulations cover infringements of intellectual property rules. While IP infringements also fall under the scope of Tunisia's Decree fixing the conditions and procedures for granting authorization for the activity of supplying internet services, intermediaries don't enjoy safe harbor provisions, and they may be subject to an order suspending their activities in case of infringement.

These rules allow for heavy government intervention and control, raising costs and potential risks for digital intermediaries. Bahrain's Copyright Law provides safe harbor provisions for network intermediaries and provide that they are not required to monitor third-party content posted on their platform. However, civil society organizations report that political content is often blocked from online platforms, and currently, entire websites, including live streaming services, are blocked. Authorities enforce the law via arrests, prosecution, and torture, forcing online forum moderators to close their platforms. (FreedomHouse 2018). Egypt's Anti-Cybercrime Law, passed in 2019, grants the government the power to block websites with content that threatens national security or the national economy. Exposing or failing to report infringing content may result in travel bans, imprisonment, and fines. In Iran, intermediaries must report any illegal content to the Committee for Determining Instances of Criminal Web Content, otherwise subject to fines or liquidation. Under UAE's Cybercrime Law of 2012, websites can be held liable for defamatory or false statements posted by third parties. In several countries, the list of restricted content is not easily accessible, making it more difficult to avoid liability.

IV. Conclusion

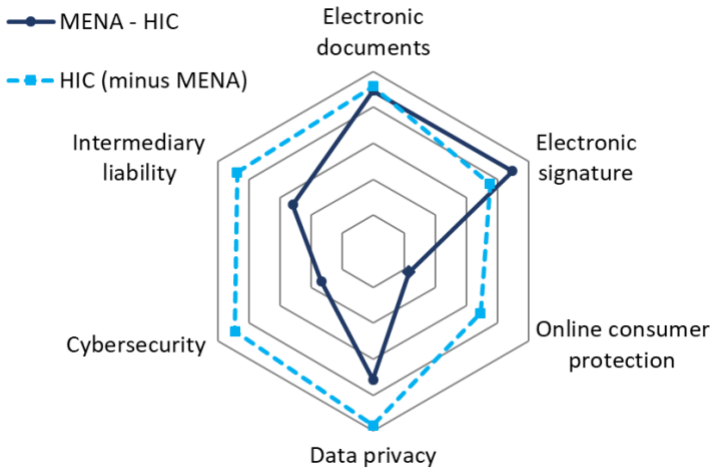
Figure 4. Digital trade regulatory readiness in MENA and comparators

A. All countries

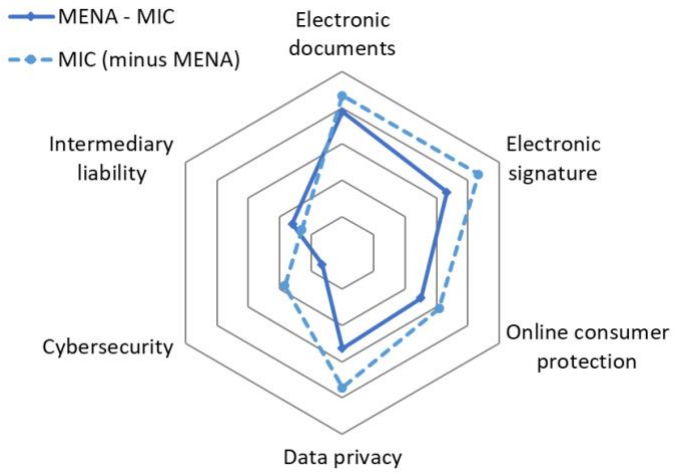


B. High Income Countries

Regulation of digital trade in MENA countries is still in its infancy, being mostly governed by general laws not originally intended for the digital era. A broad review of key regulations for digital markets in MENA suggests that the region is falling behind in establishing a modern governance framework for the digital economy. Based on a database of 40 countries, Figure 4 depicts the average progress in the regulation of digital trade in MENA, as compared to the 20 comparator countries from the rest of the world, and a subset of the three high-income countries in that sample. In general, regulation on electronic transactions (e-documents and e-signatures) in MENA countries appears broadly in line with global practices, although room for improvements remains. So do rules on intermediary liability –although mainly because the issue remains globally poorly regulated. MENA's main gap appears on the regulation of online consumer protection, data governance, and cybersecurity. The regulatory gap is particularly stark for MENA's high-income economies. Figure 4.B shows how advanced economies have attempted to keep up with the regulation of key areas of digital trade, while MENA high-income economies are lagging far behind. This gap exists also in the case of MENA's middle-income countries, although not nearly as wide as for richer economies.



C. Middle Income Countries



Lack of an adequate regulatory framework can lead to missed opportunities for digital businesses, especially those oriented to foreign markets or relying on foreign investments. For instance, apart from Israel, MENA-based firms that involve the storage or processing of personal data can find additional difficulties in doing business with European firms, as the European Union requires a level of data protection regulation that MENA currently lacks. While this requirement may not be unsurmountable –MENA companies could use EU-based servers- it does add costs and reduces the linkages of such businesses with their countries' economies. Similarly, digital platforms for e-commerce and especially content, face important risks and costs in some MENA countries for content generated and uploaded by third parties, even if the platforms have strong policies to identify and remove infringing content.

Intuitively, digital policies that have a longer history have had a greater adoption in MENA than newer digital policies. Table 18 summarizes the development status of digital markets regulations in the region. As could be expected, regulations on digital transactions, such as e-documents and e-signatures, that have more than two decades of development and have been the subject of agreed international guidelines, are the policies more frequently adopted in MENA. Except for Djibouti and the Republic of Yemen, all MENA countries reviewed have at least a comprehensive regulation for e-documents and e-signatures –although improvement and updates would be advisable for most countries. On the other side of the spectrum, regulation on online intermediary liability, which is a newer regulatory matter linked to the boom of digital platforms in recent years, has received virtually no attention from regulators and remains governed by outdated regimes inadequate to the development of digital markets. Modern data governance and cybersecurity regimes are missing in the region, with only a handful of countries having adopted modern regimes. Israel, which boasts a strong IT sector with global reach, and Qatar, seeking to become a hub in the region for IT and digital development, are the countries with the most comprehensive and up-to-date regulatory framework for data governance and cybersecurity.

Table 18: Digital trade regulatory readiness in MENA

MENA (*)	E-document	E-signature	Consumer Protection	Data governance	Cybersecurity	Intermediary Liability
Algeria	●	◕	◕	●	◔	○
Bahrain	●	◕	◑	●	◑	●
Djibouti	○	○	○	○	○	○
Egypt, Arab Rep.	◕	◑	●	○	○	◔
Iran, Islamic Rep.	◕	●	◕	◕	○	◔
Iraq	◕	◕	○	◔	○	○
Israel	◑	●	○	●	●	○
Jordan	●	●	○	◔	○	○
Kuwait	◕	◕	○	◕	○	○
Lebanon	◕	◕	●	◕	○	◕
Morocco	●	◕	●	●	◔	●
Oman	●	●	○	●	○	◕
Qatar	●	◕	◑	●	●	●
Saudi Arabia	●	●	◑	◑	○	●
Tunisia	●	◑	◕	●	◔	◕
UAE	●	●	○	◔(**)	○	○
Yemen	○	○	○	○	○	○

○ = no substantial regulation;

◔ = barebones framework or dispersed individual regulations;

◑ = comprehensive regulatory framework, but major additions or amendments needed;

◕ = comprehensive regulation in place, but small additions or updates recommended;

● = comprehensive and modern regulation in place;

(*) No available data for Libya, Palestine, and Syria. (**) Dubai provides a comprehensive data governance framework for companies under the DIFC regime.

Only a few countries have made strong efforts to keep abreast with digital regulations. Bahrain, Qatar, and Morocco feature the most comprehensive regulatory frameworks for digital markets in the region, but updates and further developments remain necessary, particularly on consumer protection and cybersecurity. On the other hand, Iraq, Jordan, and UAE have made little or no progress on digital regulation, with most regulatory solutions being severely outdated or stemming from broader frameworks not designed for current digital markets.

Some countries, like Lebanon, have recently introduced broad "e-commerce" regulations which address multiple aspects of digital markets regulations at once, from e-signature to intermediary liability matters. This kind of solution is a welcome attempt to catch up on digital regulation, which can be followed by other countries in the region with underdeveloped regulatory frameworks. These broad efforts, however, must be viewed as a first step which needs to be later complemented with individual fine-tuned regulations, ideally developed by specialized agencies in each of these fields.

MENA countries have a long way ahead in providing for a strong and comprehensive regulatory framework for digital trade. Some countries, like Qatar, Israel, and Morocco, have tried to support an export-oriented IT sector by keeping an updated regulatory framework, especially in key areas like data governance and cybersecurity. Other countries, like Lebanon, have recently jump-started a framework for digital trade by covering a range of different issues under one single legislation. Yet, regulation in most countries in the region, regardless of their level of development, still features some major loopholes that can limit consumer trust in digital markets or reduce certainty -and increase costs- for digital businesses.

The greater challenge for MENA countries remains recognizing the potential for economic growth and social development that digital trade can bring and integrating it in its economic and trade policy. From this starting point, MENA countries would benefit from introducing a standing policy for a comprehensive regulatory framework for digital trade, and a monitoring mechanism to consult with stakeholders as technologies evolve and new regulatory solutions may be needed.

Bibliography

Adobe. (2019, June). *Global Guide to Electronic Signature Law.* Récupéré sur https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/document-cloud-global-guide-electronic-signature-law-ue.pdf

AssureSign. (2019, June). *E-Sign Laws Across Borders.* Récupéré sur AssureSign: https://www.assuresign.com/e-sign-laws-across-borders/

Bartley Johns, M., Hoppe, M., Molinuevo, M., Nghardsaysone, K., & Daza Jaller, L. (2017). *Taking Advantage of E-Commerce: Legal, Regulatory and Trade Facilitation Priorities for Lao PDR.* Washington, DC: World Bank Group.

Blythe, S. (2011). *E-Commerce Law Around the World - Volume 1.* USA: Xlibris Corp.

CIGI-Ipsos. (2017). *Global Survey on Internet Security and Trust.* Centre for International Governance Innovation & IPSOS.

CipherCloud. (2017). *Global Guide to Data Protection Laws.* San Jose: CipherCloud.

Dentons. (2019, January 21). *New Lebanese law on e-transactions and data protection*. Récupéré sur https://www.dentons.com/en/insights/alerts/2019/january/21/new-lebanese-law-on-etransactions-and-data-protection

EFF. (2015, March 24). *Manila Principles on Intermediary Liability: Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation.* Récupéré sur https://www.manilaprinciples.org/

Frederick Fischer, S. (2001). Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation. *7 B.U.J.SCI & TECH. L.*, 229.

FreedomHouse. (2018, May 31). *Freedom House*. Consulté le March 25, 2019, sur https://freedomhouse.org/report/freedom-net/2018/bahrain

Gasser, U., & Schulz, W. (2015). Governance of Online Intermediaries: Observations from a Series of National Case Studies. *Berkman Center Research Publication No. 2015-5*.

Holland, A., Bavitz, C., Hermes, J., Sellars, A., Budish, R., Lambert, M., & Decoster, N. (2014). *Intermediary Liability in the United States*. Retrieved from Global Network of Internet and Society Research Centers (NoC): https://publixphere.net/i/noc/instance/noc.html

International Trade Administration. (2019, February 12). *Export.gov.* Récupéré sur Bahrain Commercial Guide: www.export.gov

Leung, H. (2019, April 2). *Time.* Consulté le April 2, 2019, sur Singapore is the latest country to propose tough legislation against fake news: http://time.com/5562501/singapore-fake-news-law-freedom-speech/

Makulilo, A. B. (2016). African Data Privacy Laws. Dans *Issues in Privacy and Data Protection.* Springer.

OECD. (2000). *Guidelines for Consumer Protection in the Context of Electronic Commerce.* Paris: OECD.

OECD. (2013). *Privacy Framework.* Paris: OECD.

OMB. (2017, January 3). *Preparing for and Responding to a Breach of Personally Identifiable Information, Memorandum for Heads of Executive Departments and Agencies.* Récupéré sur Executive Office of the President's Office of Management and Budget: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

Privacy Rights Clearinghouse. (s.d.). *Chronology of Data Breaches: Security Breaches 2005-Present.* Récupéré sur www.privacyrights.org/data-breach

UNCTAD. (2016). *Data protection regulations and international data flows: implications for trade and development.* New York and Geneva: United Nations.

UNCTAD. (2017). *Consumer Protection in Electronic Commerce: A Note by the UNCTAD Secretariat.* Geneva: United Nations.

USITC. (2017). *Global Digital Trade I: Market Opportunities and Key foreign Trade Restrictions.* The U.S. International Trade Commission.

Washington Post. (s.d.). *Hacks of OPM databases compromised 22.1 million people, federal authorities say*. Récupéré sur https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

World Economic Forum. (2019, March). *The Global Governance of Online Consumer Protection and E-Commmerce.* Récupéré sur World Economic Forum: http://www3.weforum.org/docs/WEF_consumer_protection.pdf

Annex 1: Digital Trade Regulatory Database Methodology

The Digital Trade Regulatory Readiness Assessment evaluates whether a domestic legal and regulatory framework provides answers to specific challenges brought about by digital trade. The assessment focuses on the existence of a comprehensive and modern framework that offers solutions in key matters related to digital trade, including the regulation of electronic transactions and trust-building regulation. The ground assumption of the assessment is that providing effective and transparent regulatory solutions helps foster digital trade by enhancing trust in digital markets and reducing costs related to uncertainty and ambiguity in the legal framework.

This study collects and analyzes available information on digital trade regulation assembled in a comparable manner across 40 countries, including 20 Middle East and North Africa (MENA) countries, in order to provide an analysis of the patterns of policy across countries and sectors. The five policy areas covered are electronic documentation and signature; online consumer protection; data governance; cybersecurity; and intermediary liability.

The paper seeks to facilitate the analysis of digital trade regulation, inform policymakers on recent trends and areas for reform, and provoke dialogue among stakeholders. The database, containing the index, legislative sources, and country scores, can be obtained from the authors.

About the data

The Digital Trade Regulatory Readiness database contains information on regulations that impact digital trade. There is no globally agreed definition of "digital trade". We refer to digital trade as the buying and selling of goods and services using the Internet. This includes cross-border transactions of traditional services (e.g. books) and digital services. (e.g. cloud computing).

The Assessment focuses on domestic policies that affect the supplier of the good or service as well as the consumer. It does not take into account the implementation or enforcement of the existing legislation. The purpose of this study is not to evaluate policy decisions or to cover controversial topics, but rather to assess whether governments have introduced legislation that addresses digital trade.

Countries covered in the database

The database currently includes information from a total of 40 countries, of which 20 are countries from the MENA region, and 20 are countries that represent different regions and income groups around the world (see Table A1).

Regulations covered in the database

The main focus of the database is on regulations that provide essential regulatory tools for remote transactions and promote trust among the parties to the transaction. The Regulatory Readiness Index is divided into two major topics, namely regulation on electronic transactions and trust-building regulation, with each topic further disaggregated into subtopics (electronic documentation; electronic signature; online consumer protection; data governance; cybersecurity; and intermediary liability) containing the specific variables.

Data collection process

Regulatory information for the countries covered was obtained from publicly available sources. The Assessment is based on an analysis of the texts of relevant laws and regulations available online. The data are current as of October 2019, and do not reflect any changes to the legislation after that date. For some countries, no information could be gathered, in which case this is noted in the text.

Quantification of digital trade regulations

The assessment measures the sophistication of the country's regulatory framework for digital trade. The scoring methodology uses weighted scores, reflecting the experts' assessment of the relative importance of the variables, subtopics, and topics in terms of their contribution to facilitating electronic transactions and increasing trust (see Table A2).

- Thirty-seven independent variables, ranging between 0.25 and 1 point each, add up to incremental scores per subtopic and per topic.
- The total country scores range in values between zero and 20, with zero representing an inexistent regulatory framework and 20 a comprehensive regulatory framework for digital trade.

The trust-building regulation topic was given the most weight, as the presence of legislation addressing the variables covered under this topic is deemed to show that a country has an advanced regulatory framework with regard to digital trade. Within that topic, data privacy carries the most weight, being considered as an area of great importance for the evolution of digital markets. On the other hand, the topic of regulation on electronic transactions, considered very basic, was given less weight.

Data presentation

While a score can give a quick idea of how a country's regulations stand with regard to fomenting digital trade, we believe that the information behind the number can provide better insight into the strengths and weaknesses of each regulatory framework. For this reason, the database provides details on the information gathered.

The "data" tab displays the information in a binary form, with "1" representing the presence of regulation for the specific variable and "0" the lack thereof. The "scoring" tab takes the assigned weight into account, providing the country scores for each variable as well as the total score for each country. The "sources" tab provides the legislative source for each variable, where applicable. Finally, the "index" tab provides all of the variables evaluated, the score granted to each, and the reasoning behind each variable.

Table A1. Countries covered in the database

MENA countries	Income level	Comparator countries	Region	Income level
Algeria	Upper-middle	**Albania**	ECA	Upper-middle
Bahrain	High	**Armenia**	ECA	Upper-middle
Djibouti	Lower-middle	**Bangladesh**	SA	Lower-middle
Egypt, Arab Rep.	Lower-middle	**Burkina Faso**	SSA	Low
Iran, Islamic Rep.	Upper-middle	**Canada**	NA	High
Iraq	Upper-middle	**Colombia**	LAC	Upper-middle
Israel	High	**France**	ECA	High
Jordan	Upper-middle	**Honduras**	LAC	Lower-middle
Kuwait	High	**Indonesia**	EAP	Lower-middle
Lebanon	Upper-middle	**Kazakhstan**	ECA	Upper-middle
Libya	Upper-middle	**Kenya**	SSA	Lower-middle
Morocco	Lower-middle	**Korea, Rep.**	EAP	High
Oman	High	**Kyrgyzstan**	ECA	Lower-middle
Palestine	Lower-middle	**Malaysia**	EAP	Upper-middle
Qatar	High	**Mexico**	LAC	Upper-middle
Saudi Arabia	High	**Moldova**	ECA	Lower-middle
Syrian Arab Republic	Low	**Pakistan**	SA	Lower-middle
Tunisia	Lower-middle	**Senegal**	SSA	Lower-middle
United Arab Emirates	High	**Tanzania**	SSA	Low
Yemen, Rep.	Low	**Vietnam**	EAP	Lower-middle

Table A2. Digital Trade Regulatory Index

	Variable	Score
	Regulation on electronic transactions	**4**
	Electronic documentation	**2**
1	Electronic documents are legally valid	1
2	Specific provision provides detail on admissibility of e-documents as evidence	0.5
3	The law is technology neutral regarding the storage of e-documents	0.5
	Electronic signature	**2**
4	Electronic signatures are legally valid	0.5
5	Certificates issued by a qualified certification authority (CA) or using specific technology are recognized same legal status as handwritten signature	0.5
6	Digital signatures with a valid certificate are afforded a rebuttable presumption, regardless of certification provider or technology used	0.5
7	Certification authorities may be private parties, in addition to public entities.	0.5

Trust-building regulation			**12**
	Online consumer protection		**4**
8		Framework explicitly addresses online consumer protection	0.5
		Online information disclosure requirements:	
9		Full business address of merchant	0.25
1		Full description of the product or service	0.25
11		Information about delivery and/or payment	0.25
12		Information about complaint handling	0.25
13		Existence of the right of withdrawal	0.5
14		No need to provide a reason for withdrawal	0.5
15		Availability of an online dispute resolution mechanism	0.5
16		Refund available as an option for redress	0.5
17		Additional alternatives for redress, such as repair, replacement, or partial refund	0.5
	Data privacy		**5**
18		Framework explicitly addresses online personal data privacy protection	1
19		Special rules for the treatment of sensitive personal data during processing	0.5
		Legal basis for data collection and processing:	
20		Consent by data subject	0.25
21		Performance of a contract to which the customer is party	0.25
22		Compliance with a legal obligation to which the controller is subject	0.25
23		Legitimate interests pursued by the controller or by a third party	0.25
24		Data subject's right to electronic data access and data deletion	1
25		Explicit rules on cross-border data transfers	0.5
26		Where data is required to be stored domestically, such requirement does not prevent from transferring a copy of it abroad (subject to other conditions if necessary)	1
	Cybersecurity		**3**
27		Data encryption required	0.5
28		Internal data protection policy required	0.5
29		Appointment of a data manager required	0.5
30		Risk assessment procedures required	0.5
31		Data breach notification requirements	0.5
32		Supervisory authority in charge of enforcement	0.5
Platform Regulation			**4**
	Intermediary liability		**4**
33		Framework explicitly addresses online intermediary liability	0.5

34		Safe harbor provisions exist to shield online intermediaries from liability	1
35		Infringements related to intellectual property are covered	1
36		Notice and stay-down procedures required	1
37		An order from a judicial authority is required for content restriction	0.5
		Scoring TOTAL	**20**