The Extraterritorial Impact of EU Digital Regulations: How Can the EU Minimise Adverse Effects for the Neighbourhood?

In recent years, the European Union (EU) has taken significant steps to harmonise its data privacy laws. This includes the implementation of the General Data Protection Regulation (GDPR) in 2018, alongside the introduction of the Digital Markets Act (DMA), Digital Services Act (DSA), and the Data Act. These regulatory changes have not only unified the digital landscape within the EU but have also extended their impact beyond its borders, posing significant challenges for neighbouring countries. These nations are now grappling with increased trade barriers stemming from complex data compliance and governance requirements.

Considering these developments, this policy paper explores the EU's digital trade relations with its neighbours. It assesses how these countries have adapted to existing global data regulation models. This paper offers an overview of the existing provisions in trade and other agreements related to data trade between the EU and its neighbouring countries and explores potential avenues for boosting trade by means of the EU granting data adequacy status. Additionally, it puts forth recommendations for strengthening digital integration between the EU and its neighbouring states, with the aim of reinforcing regional ties and reducing the likelihood of these countries turning towards alternative global influences.

ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

BertelsmannStiftung

1. Global Data Regulation Models: Impact on Digital Trade

Although regulations governing the processing and protection of personal data vary among countries, we can identify three distinct models: the United States' open model, which allows for the free flow of data; China's closed model,[1] which is characterised by strict government controls; and the EU's middle-ground model, which incorporates conditional data transfers and regulatory safeguards. Each of these data models encompasses two key aspects of data regulation: one pertains to rules governing the cross-border transfers of personal data, while the other focuses on rules governing the domestic processing of personal data (see TABLE 1). As new regulations extend to non-personal data and AI, a similar divergence between the EU and the US becomes apparent: whereas the EU adopts a "conditional" approach, the US is less restrictive.[2]

TABLE 1: **Main features of different data models**

	Cross-border data transfers	Domestic data processing
Open Transfers and Processing Model	Self-certification; self-assessment schemes; ex-post accountability; trade agreements and plurilateral/bilateral arrangemnets as only means to regulate data transfers.	Lack of comprehensive data protection framework; lack of informed consent; privacy as a consumer right.
Conditional Transfers and Processing Model	Conditions to be fullfilled ex-ante, including adequacy of the recipient country, binding corporate rules (BCR), standard contract clauses (SCCs,) data subject consent, codes of conduct, among others.	Wide data subject rights; data subject consent; right to access, modify and delete personal data; establishment of data protection authorities (DPAs) or agencies; privacy as fundamental human right.
Limited Transfers and Processing Model	Strict conditions including bans to transfer data cross border; local processing requirements: ad hoc government authorization for data transfers; infrastructure requirements; ex-ante security assessments.	Extensive exceptions for government access to personal data; privacy vs security and social order.

Source: Authors

BertelsmannStiftung

FIGURE 1 characterises EU neighbouring countries according to the different data models outlined above. It shows that EU neighbours like Morocco, Ukraine and the Western Balkans align with the EU model. Conversely, nations such as Egypt, Libya, Jordan and Lebanon tend to follow the more open model, while Algeria and Tunisia align with the closed model.

FIGURE 1: **Mapping of EU neighbouring countries according to different data models**

Note: Countries following the open model are indicated in green; those following the closed data model are shaded red, and those following the EU data model are shown in blue. The EU countries that have adopted the EU digital regulations are shown in light blue, while other neighbouring countries are shown in dark blue to indicate that they follow the EU model. Countries for which no data is available are shaded grey.

Source: Authors; Graphic powered by Bing © GeoNames, Microsoft, TomTom

BertelsmannStiftung

1 In 2021, China issued a regulation on recommendation algorithms to prevent misuse. China has three key regulations on algorithms: the 2021 regulation addressing the recommendation of algorithms, the 2022 rules for synthetically generated content, and the generative AI regulation. These regulations set out requirements for disclosure, model testing mechanisms and technical performance standards. The 2021 regulation on recommendation algorithms has become a precedent for setting global standards, as it is the most comprehensive regulation requiring transparency about how the algorithm works. However, the degree of ex-ante and self-imposed constraint on these inputs, in line with the CCP's objectives, should not be underestimated.

2 See also Bradford, A. (2023). Digital Empires. The Global Battle to Regulate Technology. Oxford University Press.

Research conducted by Martina Francesca Ferracane and Erik Van der Marel reveals intriguing trade patterns among country pairs that align with specific data models. Specifically, when both countries adopt the closed data model, they tend to exhibit negative trade correlations. Conversely, country pairs adhering to the open and middle-ground models generally experience an uptick in their digital services trade.[3]

This research suggests that the EU's trade with neighbouring countries that follow its conditional data flow model should be robust. However, contrary to expectations, these countries, on average, engage in less trade than those adhering to the open model.[4] One potentially significant factor contributing to this disparity is the restrictive nature of the EU's model, which stands in contrast to the more permissive US approach to data flows. The EU model's insistence on conditional data transfers, which requires compliance verification, hinders the spontaneous trade often observed in open data flow regimes. Consequently, these associated restrictions and implementation costs contribute to trade reductions.

Indirect evidence of these trade losses can be drawn from the rise in digital trade, which has shown an increase ranging from 6% to 14% among countries that have obtained adequacy status from the EU.[5] This trend implies a potential reduction in trade costs of up to 9%. Moreover, a network effect is discernible, as countries with adequacy status also benefit from the EU's adequacy decisions with other countries such as the United States. Research shows that approximately 7% of digital value-added trade has been redirected from countries lacking adequacy status or from domestic markets towards those integrated into the EU's adequacy network.[6]

2. Digital Trade and Regulatory Alignment: Shaping the EU's Neighbourhood Relations

The insights from Chapter 1 underscore the significance of regulatory alignment in boosting digital trade between the EU and its neighbouring countries. For those neighbouring states that are either on the path to EU membership or engaged in accession negotiations, adopting the EU's acquis communautaire naturally results in harmonising their national laws with EU standards. However, given the prolonged duration of accession negotiations, the EU should also explore intermediate measures for these countries, such as granting adequacy.

For those countries that cannot join the EU, there are two primary pathways: the first involves integrating digital standards into trade and association agreements, as exemplified by the agreements with Armenia and the Deep and Comprehensive Free Trade Areas (DCFTA) with Georgia, Moldova and Ukraine; the second involves the EU Commission recognising equivalent data protection levels, which other countries can achieve through different means, as outlined in Art. 45 of the GDPR,[7] and subsequently granting adequacy.

Currently, aside from Israel, no other neighbouring country has secured an adequacy agreement with the EU. However, existing trade and association agreements between the EU and its neighbours include numerous relevant data handling provisions, some of which carry legal obligations. These provisions could serve as a basis for further alignment towards data adequacy, particularly for those southern countries that cannot join the EU. An overview of these binding and non-binding digital and data-related provisions can be found in TABLE 2.

3 Ferracane, M. & Van der Marel, E. (2021). Regulating Personal Data: Data Models and Digital Services Trade. https://documents1.worldbank.org/curated/en/890741616533448170/pdf/Regulating-Personal-Data-Data-Models-and-Digital-Services-Trade.pdf

4 Ibid.

5 When the European Commission adopts an adequacy decision it "certifies that the data protection regime of the trading partner is overall equivalent to the EU." The aim of an adequacy decision is to ensure equitable treatment in the processing of personal data, whether it occurs within the EU or outside of it, between the EU and its trading partner. See: Ferracane, M., Hoekman, B., Marel, E. and Santi, F. (2023.) Digital Trade, Data Protection and EU Adequacy Decision. Robert Schuman Centre for Advanced Studies. https://cadmus.eui.eu/bitstream/handle/1814/75629/RSC%20WP%202023%2037_V5.pdf?sequence=1&isAllowed=y; Regulation (EU). 2016/679 of the European Regulation of the European Parliament and the Council. Art. 3. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

6 Ferracane, M. Hoekman, B., Marel, E. and Santi, F. (2023). Digital Trade, Data Protection and EU Adequacy Decisions. Robert Schuman Centre for advanced Studies. https://cadmus.eui.eu/handle/1814/75629

7 Regulation (EU) 2016/679 of the European Regulation of the European Parliament and the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

TABLE 2: **Data and digital provisions of EU agreements with neighbouring countries**

Agreement title	Year of entry	Type of non-binding provisions	Type of binding provisions
EU Armenia CEPA	2018/2021[8]	Includes the protection of personal data/ personal information	No customs duties must be imposed on electronic transmissions and digital products
			The adoption or continued maintenance of a legal framework that adheres to international standards in terms of providing for the protection of the personal information of users engaged in digital trade
			Acknowledges the importance of ensuring compliance with personal information protection measures and verifying that any limitations on the cross-border movement of personal information are both necessary and proportionate to the associated risks
			The agreement includes limitations on and exceptions to copyright and related rights
			The agreement contains provisions that explicitly address trade secrets or similar forms of protection for undisclosed information and data
Bosnia and Herzegovina EC SAA	2008/2015[9]	Includes the protection of personal data/information	The agreement contains provisions that explicitly address trade secrets or similar forms of protection for undisclosed information and data
Algeria EC Euro-Med Association Agreement	2005/2015[10]		Includes protection of personal data/information
			The agreement contains data protection provisions that acknowledge limitations on: data collection, choice and quality; specifying purpose, restricting use, ensuring security measures, transparency, individual participation, accountability, non-discrimination and compatibility
EC Georgia DCFTA	2016	Includes the protection of personal data/information	No customs duties can be applied to electronic transmissions and digital products.
		The adoption or continued maintenance of a legal framework that adheres to international standards in terms of providing for the protection of the personal information of users engaged in digital trade	Recognises the need of ensuring compliance with personal information protection measures and ensuring that any restrictions on cross-border flows of personal information are essential and reasonable to the risks presented.
			The agreement includes limitations on and exceptions to copyright and related rights
EC Moldova DCFTA	2014/2016[11]	Includes the protection of personal data/ information	No customs duties must be imposed on electronic transmissions and digital products
			Adoption or maintenance of a legal framework that provides for the protection of the personal information of the users of digital trade following international standards
			The agreement includes limitations and exceptions to copyright and related rights
EC Ukraine DCFTA	2017	Includes protection of personal data/ personal information	No customs duties must be imposed on electronic transmissions and digital products
		Adoption or maintenance of a legal framework that provides for the protection of the personal information of the users of digital trade following international standards	Adoption or maintenance of a legal framework that provides for the protection of the personal information of the users of digital trade following international standards
			The agreement includes limitations and exceptions to copyright and related rights
			The agreement includes provisions that address patents for computer software

Note: Non-binding provisions are commitments in which one party cannot compel the other party to adhere to. These commitments involve a promise to make "best efforts" to comply with a clause or a concept, but the agreement's dispute mechanism cannot be used to enforce a claim of non-compliance.

Source: TAPED database

BertelsmannStiftung

8 EU Armenia CEPA has been provisionally applied since June 2018 and formally entered into force on March 2021.
9 Bosnia and Herzegovina EC was signed in 2008 and entered into force in 2015.
10 EU Algeria Association Agreement was signed in April 2002 and entered into force in September 2005.
11 The EC Moldova Association Agreement was signed in 2014 and has been in full effect since 2016.

The likelihood of other countries in the Southern Neighbourhood obtaining an adequacy regulation with the EU appears slim at this point. While enacting similar data regulation laws may be feasible for these countries, the real challenge lies in effectively applying and monitoring these regulations. EU digital regulations, such as the GDPR, require substantial governance capabilities to ensure proper compliance, and without this proof, the EU cannot grant adequacy status.

For instance, Jordan[12] and Lebanon currently lack data protection laws and independent data protection authorities. In the case of Lebanon, there is a proposed law that would not only enhance data protection but also establish a Personal Data Protection Board.[13] Another group of countries, including Armenia (2020),[14] Algeria (2018),[15] Türkiye (2016)[16] and Egypt (2020),[17] has recently enacted their initial laws concerning personal data protection. Morocco and Tunisia have older data protection regulations in place. Tunisia has introduced a draft law[18] on personal data protection, aligning with Europe's GDPR, to update its 2004 law, and has also sought adequacy status from the EU. Morocco's Data Protection law was passed in 2004 and subsequently amended in 2009, prompting the country to apply for adequacy, though this request is still pending.[19] While of the mentioned countries have not yet actively sought an adequacy decision from the EU, many are in the process of taking the necessary steps that could potentially lead to such a request for data protection adequacy in the future.[20]

3. Digital Trade Patterns: Analysing the EU's Neighbourhood Digital Trade

The growth of digital trade between the EU and its neighbouring countries depends not only on existing legal frameworks, but also, and perhaps more importantly, on the level of economic development in each respective country. Furthermore, the diversification of their services trade portfolio and the range of digital trade goods they can offer play significant roles in shaping this trade dynamic.

This chapter presents an analysis of the current state of digital services trade between the EU and its neighbouring states. TABLE 3 examines the share of digital services within the overall service exports of EU neighbouring countries, which encompasses a wide range of digital-intensive industries. These industries include insurance and pension services, financial services, intellectual property charges, telecommunications, computer and information services, and a variety of other business, cultural and recreational services.

TABLE 3: **Share of digital services in total services exports (% and in million USD)**

Country	Percentage share	Export value
Israel	67.4	31354.9
Libya	53.5	660.5
Serbia	51.3	4057.3
Ukraine	48.5	7755.0
Belarus	42.0	3719.2
Lebanon	40.1	1777.1
Algeria	39.5	1560.3
Morocco	38.2	5368.1
North Macedonia	37.3	803.1
Moldova	37.2	679.8
Palestine	36.0	1328.0
Kosovo	34.6	834.2
Azerbaijan	33.5	1138.0
Armenia	31.2	641.8
Georgia	28.9	661.3
Bosnia and Herzegovina	22.5	623.5
Egypt	20.3	4811.2
Jordan	19.1	784.5
Tunisia	17.2	1198.9
Türkiye	16.2	8713.3
Montenegro	14.8	262.2
Syria	12.5	84.0
Albania	8.3	326.9

Note: Data is from the latest available year, 2021. Source: OECD-WTO Balanced Trade in Services dataset (BaTIS) and author's calculations

Source: OECD-WTO Balanced Trade in Services Dataset (BaTIS) and author's calculations | BertelsmannStiftung

Israel, the only country of the region with which the EU has an adequacy agreement, stands out as the frontrunner with the highest percentage share of digital services at

12 Accessnow (2023). Policy Brief: What's wrong with Jordan's data protection law and how to fix it. www.accessnow.org/publication/jordan-data-protection-law/
13 Personal Data Protection Act of 2021. Ministry of Digital and Entrepreneurship of Jordan. https://modee.gov.jo/Ar/NewsDetails/%D9%82%D8%A7%D9%86%D9%88%D9%86_%D8%AD%D9%85%D8%A7%D9%8A%D8%A9_%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA_%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D9%91%D9%8E%D8%A9_%D9%84%D8%B3%D9%86%D8%A9_2021%D9%85
14 Data Guidance (2022). Armenia – Data Protection Overview. www.dataguidance.com/notes/armenia-data-protection-overview-0#:~:text=Article%2015%20of%20the%20Personal,to%20whom%20the%20personal%20data
15 Data Protection Africa (2022). Data Protection Fact Sheet. https://dataprotection.africa/algeria/#:~:text=DPA%20legislation%3A%20Law%20No.,the%20protection%20of%20personal%20data
16 Personal Data Protection Law No. 6698 (KVKK). www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law
17 ILO (n.d.) Egypt: General Provisions www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=111246&p_count=7&p_classification=01#:~:text=Law%20151%2F2020%20on%20the%20Protection%20of%20Personal%20Data.,-Country%3A&text=Abstract%2FCitation%3A,appoint%20a%20-Data%20Protection%20Officer
18 DLA Piper Intelligence (2023). Data Protection Laws from the world. Tunisia. www.dlapiperdataprotection.com/index.html?t=law&c=TN
19 Chenaoui, H. (2018). Moroccan data protection law: Moving to align with EU data protection? https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection/
20 A more detailed overview of the state of play of the agreements and relevant provisions on a country basis is provided in Annex 3.

67.4% and an export value of USD 31,354.9 million. This highlights Israel's robust position in the digital services sector. Other countries, such as Belarus, Libya, Serbia and Ukraine also show a high percentage of digital services in their total services exports, with shares ranging from 42.0% to 53.5%. Similarly, digital services comprise a significant share in Algeria, Lebanon and Morocco.

TABLE 4: **Share of digital services exports to the EU as a percentage of total services exports (% and in million USD)**

Country	Percentage share	Export value
Bosnia and Herzegovina	68.0	424.1
Serbia	50.1	2031.1
Morocco	48.7	2613.8
Albania	46.9	153.5
Türkiye	45.8	3990.0
North Macedonia	44.8	359.8
Kosovo	44.7	373.2
Syria	44.6	37.4
Moldova	42.8	291.3
Libya	40.6	268.3
Algeria	35.7	557.4
Ukraine	33.7	2611.8
Egypt	33.4	1607.7
Montenegro	33.4	87.5
Armenia	31.7	203.6
Tunisia	31.2	373.6
Azerbaijan	30.7	349.8
Israel	28.6	8953.9
Georgia	27.7	183.3
Belarus	24.8	922.6
Lebanon	22.3	395.9
Jordan	19.0	149.1
Palestine	10.7	142.4

Note: Data is from the latest available year, 2021.

Source: OECD-WTO Balanced Trade in Services dataset (BaTIS) and author's calculations | BertelsmannStiftung

TABLE 4 shows the exports of digital services to the EU relative to each country's total services exports, along with their respective export values. The data reveals notable patterns. For example, Bosnia and Herzegovina stands out with an impressive share of 68.0% in digital services exports to the EU that amounts to an export value of USD 424.1 million, indicating a marked reliance on the EU market. Serbia, Morocco, Albania, and Türkiye also show notable integration with the EU, as their digital services exports to the EU make up between 45.8% and 50.1% of their total services exports. This trend of strong connections to the EU market is also seen in the examples of North Macedonia, Kosovo and Syria, each with over 40% of their services exports dedicated to digital services for the EU market. In contrast, Israel, despite featuring a lower relative share of 28.6% in digital services exports to the EU, still plays a significant role with an export value of totalling $8,953.9 million.

Insights into the export of digital services to the EU reveal an intriguing dynamic: certain countries, despite their substantial global digital services exports, engage in proportionally less trade with the EU. For example, Ukraine directs only 33.7% of its digital services exports to the EU, even though these services comprise 48.5% of the country's global exports. This gap highlights Ukraine's significant trade relationships with non-EU partners and points to opportunities for expanding digital services trade between the country and the EU. Similar patterns can be observed in countries like Belarus, Lebanon and Libya, although these countries' trade relationships with the EU may be influenced more substantially by geopolitical factors.

In addition to these broader issues, it's crucial to consider as well the diversity in the digital trade capabilities and characteristics of the EU's neighbouring countries. Deeper trade integration could enable these neighbouring countries to further diversify their existing exports. TABLE 5 sheds light on the specific types of digital services these countries trade with the EU. The data on digital services exports to the EU reveals distinct trends among North African countries, indicating a less diversified approach compared to other neighbouring regions. These countries primarily focus on a limited range of key commodities, which narrows the breadth of their services trade with the EU. This situation leads to competition among some neighbouring countries for a share of the EU market. For instance, Morocco finds itself in competition with recent EU members from Eastern Europe, as evident from trade complementarity indexes. It's worth noting that, despite the challenges associated with diversification, Africa has witnessed significant growth in services trade, including digital services, in recent years.[21]

21 For a closer look at the trade characteristics and patterns of the digital sector in various EU neighbourhood countries, please refer to Annex 2.

TABLE 5: **Composition of digital-enabled services exports to the EU (in million USD)**

Country	Telecommunications, computer and information services	Insurance and pension services	Financial services	Charges for the use of intellectual property	Other business services	Personal, cultural and recreational services
Israel	2739	324	760	340	2632	106
Türkiye	2254	796	537	1356	3143	240
Ukraine	1197	43	162	461	1696	67
Egypt	849	432	315	174	1507	42
Morocco	614	73	93	99	641	33
Serbia	399	35	55	251	877	17
Bosnia and Herzegovina	106	41	104	48	333	5
Kosovo	92	39	43	34	117	4
Albania	82	13	6	84	22	2
North Macedonia	68	63	10	58	154	5
Algeria	15	0.01	12	15	632	5
Belarus	528	17	19	32	319	9

Note: The data presented is from 2021, the latest available year. "Other business services" encompass a range of services, including but not limited to research and development services, professional and management consulting services, as well as technical, trade-related and various other business services.

Source: OECD-WTO BaTIS and author's calculations

BertelsmannStiftung

4. Mitigation Measures the EU Could Pursue

Europe has begun exploring new approaches to data and digital policies in agreements with partner countries. These new trade, technology and digital partnerships, such as the Trade and Technology Councils with India[22] and the United States,[23] aim to facilitate improved coordination on various data regulations. This endeavour has the potential to open doors to agreements on specific trade issues, including measures related to data localisation. Some of these trade agreements, such as those with Canada, Japan and the UK,[24] go beyond the norm by incorporating robust provisions on data and digital policies. This heightened level of commitment provides greater market access security for operators and, in some cases, has led to adequacy decisions following these negotiations and agreements.

However, few of these agreements offer specific guidance on how data regulations should operate. None of the agreements include provisions on AI and industrial data regulations or address how partners should cooperate to prevent the emergence of new regulations that could create new trade barriers. In light of the rapidly changing landscape in data and AI regulation, it would be beneficial for the EU to engage its partners more actively in the process of crafting new regulations. This engagement should involve tailored implementation designed to meet each partner's unique needs, particularly in the context of developing and emerging countries.

The fields of data and AI regulation are evolving swiftly, and even the most recent agreements do not reflect the current landscape of regulations adequately. Furthermore, including provisions in agreements does not automatically guarantee a reduction in friction. To facilitate smoother trade integration, practical mechanisms and processes are required to address regulatory complexities and burdens, all while staying true to the overall objectives. A case in point is adequacy, where provisions on data privacy regulations are present in trade agreements, but the free flow of personal data can only occur once the European Commission grants adequacy status to a partner country.

The neighbouring countries covered in this policy brief present additional challenges for seamless digital trade integration. Few of them have developed regulatory frame-

22 European Commission (2023). First EU-India Trade and Technology Council focused on deepening strategic engagement on trade and technology. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2728
23 European Commission (2023). EU-US Trade and Technology Council. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en
24 European Commission (2023). Access2Markets. https://trade.ec.europa.eu/access-to-markets/en/non-eu-markets

works and supervisory institutions in the realm of data, AI and embodied services that match the scale and scope of the EU's approach. While there has been some convergence in data privacy and certain data-processing regulations, Israel is the only country to have achieved adequacy status within the EU, and substantial frictions continue to impede closer engagement with other countries. Moreover, some economies in this group are relatively underdeveloped and face broader governance issues, which makes it difficult for them to achieve regulatory alignment with the EU. Recognising these alignment challenges, it's clear that divergent regulatory regimes will continue to hinder the flow of digital trade. For many of these countries, new alignment strategies that create more favourable conditions for integrating into the EU's digital market are therefore necessary.

As the EU continues to refine its policies regarding data and the portability of digital services, it should be mindful of potential challenges stemming from certain regulations. It should intensify its efforts to mitigate these challenges for neighbouring countries while upholding its regulatory objectives. The EU holds a prominent global position in digital trade, being the leader in exports of digitally deliverable services with a value of $770 billion in 2022, surpassing the United States at $632 billion and China at $200 billion in exports.[25] Given these economic interests, the EU is keen on maintaining trade openness and enhancing market access. Equally important is the EU's strategic interest in fostering close collaboration with its neighbouring countries, allowing them to align with Europe's digital economy and potentially bolstering its economic influence through greater integration.

In this chapter we will explore five distinct approaches to mitigate the challenges faced by EU neighbouring countries due to recent EU digital regulations. They are all based on the assumption that the EU will retain the substance of its existing regulations. First, the EU could reevaluate its existing bilateral agreements with a focus on updating and improving provisions related to data and digital regulations. Additionally, digital partnerships could be extended to neighbouring countries, with an emphasis on tailoring these partnerships to the unique circumstances and capabilities of each specific country. Second, by expanding adequacy and other mutual recognition mechanisms, the EU can provide more effective pathways for other countries to align with the EU regulatory framework. The third option, though unconventional, involves establishing agreements with countries that allow their companies to utilise EU supervisory bodies for regulatory compliance – a process akin to extending institutional authority to partner countries. Fourth, the EU can establish mechanisms that are not conditioned on regulatory cooperation with other countries but which help firms in other countries to "declare" compliance. Finally, the EU can assist its own firms by developing mechanisms to mitigate liability risks when they engage in data operations within neighbouring jurisdictions.

None of these policy options can comprehensively address all the challenges arising from diverse data and digital regulations affecting digital trade. Should the EU opt for a constructive and cooperative approach towards its neighbours and seek to facilitate their integration into the EU's digital market, it must engage with these countries and their businesses by combining various policy options.

POLICY OPTION 1

Modernising existing agreements

The EU could alleviate the consequences faced by the EU neighbourhood by formulating digital policy agreements aimed at promoting increased trade and reducing obstacles for these countries. The analysis in chapter two pointed to obvious problems in the current set of agreements between the EU and its neighbours. First, the existing provisions related to data and digital regulations are generally insufficient. Second, these agreements fail to keep pace with the rapid advancements in technology and the introduction of new regulations. Consequently, there is a need to modernise these agreements to better align them with the actual dynamics of cross-border digital integration, taking into account both opportunities and challenges.

Modernising the agreements would involve incorporating fundamental provisions for digital trade. While it may be challenging to establish detailed operational rules for data regulations through broader bilateral agreements, there are basic concepts of digital trade that are still missing in many of these agreements. Some agreements are more robust than others, and harmonising the weaker ones with the stronger ones would improve the conditions for digital integration. Initiating new digital partnerships with neighbouring countries of the EU could also support and facilitate this modernisation process. These agreements and digital partnerships also play an important role in fostering trust and encouraging relevant regulatory bodies to cooperate. The EU would be well-advised to pursue a more equitable approach in this process.

In addition, the EU has begun to take a novel approach to international cooperation on digital issues. In 2022, it initiated digital partnerships with Japan, South Korea and Singapore. These partnerships differ from conventional trade agreements by covering a wide range of topics such as privacy, cybersecurity and data governance, as well as addressing digital trade issues like paperless transactions and online consumer protection. These digital partnerships also aim to serve as a blueprint for future cooperation

25 Köhler-Suzuki, N. (2023). Mapping the EU's digital trade: a global leader in plain sight? Jacques Delors Institute. https://institutdelors.eu/wp-content/uploads/2023/08/PP293_Maping-EU-digital-trade_Kholer-Suzuki.pdf

on issues a range of matters extend beyond trade, such as coordination in crucial areas like semiconductors, 5G networks, artificial intelligence and quantum technology. Extending this initiative of digital partnerships to the EU's neighbourhood countries could bolster and expedite the aforementioned modernisation process, thereby promoting closer integration and reducing trade costs for these countries. It's worth noting, however, that the existing digital partnerships are established with highly developed countries, and any expansion of this initiative to the EU's neighbourhood should be tailored to the specific regulatory framework, level of development and capacities of each neighbouring country.

POLICY OPTION 2

Adequacy, other mutual recognition mechanisms and standards

The GDPR has a mechanism aimed at simplifying alignment with the EU system in the realm of data privacy. When a country is granted adequacy status, personal data can flow freely between the EU and that country. Essentially, this means that the EU recognises the other country's regulations as being similar to its own, and it deems that country's oversight institutions competent and authoritative. In cases where adequacy has not been granted, companies engaged in cross-border personal data transfers must resort to using standard contractual clauses and binding corporate rules, which can be expensive and time consuming. This approach is usually only viable for very large firms with substantial data operations.

Two noteworthy observations are pertinent to our discussion about the efficacy of adequacy-type approaches for various regulations crucial to digital markets. First, the GDPR stands out as one of few data regulations featuring a specific mechanism that enables other countries to "dock" with the EU regulation and market standards. Most other regulations lack such mechanisms. Second, achieving something akin to mutual recognition requires working with standards and the practical implementation of regulatory measures. In many domains of emerging data regulations, progress in this regard remains inadequate.

Currently, apart from Israel, no other country in the EU neighbourhood has obtained adequacy status from the EU. It will undoubtedly take time before other countries in the region reach a point where adequacy can be seriously considered. Similarly, as the EU introduces new regulations concerning AI and industrial data, the prospect of mutual recognition between the EU and most neighbouring countries remains distant. Most of these countries are pursuing different approaches to these regulations, and the same challenges that complicate adequacy in the GDPR context are likely to hinder necessary progress for mutual recognition in these emerging regulatory areas.

However, through the development of more standards, the EU could pave the way for novel methods of policy recognition. In the absence of standards, mutual recognition can often prove challenging, as it requires the intricate evaluation of variations and similarities in the formulation of laws and regulations. Nevertheless, even when there are significant differences in actual regulations, standards can often exhibit close resemblances, potentially facilitating types of recognition that reduce integration costs. In other words, by establishing operable standards or acknowledging private standards, the EU could facilitate cross-border digital integration.

The EU has the opportunity to tap into these potential trade opportunities with its neighbouring countries. As the EU contemplates new regulations on non-personal data (the Data Act) and important regulations related to embodied data flows (e.g., through the AI Act), it is crucial to devise policies and mechanisms that make it easier for neighbours to rely on EU data and digital service markets. To gain a better understanding of their readiness to align with EU regulations, the EU should engage these countries more actively in the policymaking process from the beginning.

POLICY OPTION 3

Lending institutional authority

A different and unconventional approach would involve offering neighbouring countries the option for an EU authority to act as the effective regulator of a data operator or firm within their jurisdictions. Under such circumstances, non-EU firms in partner countries could opt to operate under the laws and supervision of an EU member state or an EU regulatory body in a defined and limited area of regulation. Obviously, implementing such an approach would require cooperation on governmental and legal levels, granting the "lending" authority access to compliance structures and courts. In this scenario, a non-EU firm in a partner country would enjoy the freedom to conduct business within the EU single market on par with EU companies. This would result in reduced trade and compliance costs, enhancing the conditions for non-EU firms to integrate more deeply into the EU digital market.

Although historical examples exist where one country, backed by strong and trusted institutions, extends the use of their institutions to another country, this policy approach can be contentious due to its implications for national sovereignty. Nonetheless, there are practical precedents that can serve as inspiration for such a development. For instance, when the EU establishes a standard, firms in other countries have the voluntary choice to adopt that standard, irrespective of the regulations and standards applicable in their home countries. Many companies in the EU's neighbouring countries that work together with large multinational firms already adhere to different regulatory and standard practices compared to firms primarily

focused on domestic markets. The "Brussels effect" within the EU demonstrates that non-EU companies often apply EU regulations, such as the GDPR, across all of their operations, even when less stringent regulations are available outside the EU. In both instances, the institutional authority of the EU extends beyond its borders.

Importantly, this model holds particular appeal for countries on the path to EU accession or those engaging with the EU in a DCFTA. Accession countries are required to adopt EU regulations concerning data and digital markets before their accession, which means that national firms will inevitably be subject to EU regulations. Analogous to the process of full accession, which involves multiple intermediary agreements resulting in the subordination of national laws, regulations and institutions to the EU, the EU could make this approach available for data and digital regulations as well. Likewise, many areas of regulatory cooperation within the DCFTAs rely on extensive collaboration between regulatory institutions.

POLICY OPTION 4

Declaration of compliance

A standard method of ensuring regulatory compliance for several products involves conformity assessments. These assessments result in an independent body issuing a declaration of conformity to a company that intends to place a product on the market. While this approach is not without its challenges, it proves to be a cost-effective way to ensure adherence to specific regulations across sectors without creating barriers to trade. Irrespective of where a product is manufactured or the operations carried out, a company seeking access to the EU market can obtain a conformity declaration and collaborate with EU-based business partners. Alongside standards and their development, conformity declarations play a pivotal role in facilitating international trade.

However, when it comes to data and digital regulations, the practice of conformity faces unique challenges. Few of the EU's recent data regulations incorporate formal conformity as a means of compliance. Of course, not all data and digital regulations can accommodate conformity declarations, but many have provisions that could be effectively managed by firms to demonstrate compliance. Notably, the proposed AI Act introduces a mechanism for conformity assessments to declare compliance with its rules. In principle, this approach could serve as a model for other regulations that grapple with how foreign operators should demonstrate compliance with EU regulations.

A complicating factor, especially with regard to the AI Act, is that the introduction of an AI product into the EU market inherently involves the underlying data for the AI application. This issue intersects with the requirements set forth by the GDPR, particularly regarding Data Protection Impact Assessments (DPIA) if the data in question qualifies as personal data. The history of DPIAs in complex cross-border supply chains has been marked by uncertainty, a situation exacerbated by duplicated and sometimes conflicting rules among different EU data protection authorities. The associated costs and risks often dissuade many companies from engaging in cross-border data integration.

In light of these challenges, a broader observation is that the EU could streamline the process of declaring conformity and incorporate conformity mechanisms into more of its regulations. For instance, the rules surrounding DPIAs are not always clear, especially concerning the allocation of roles within complex data value chains. Even though DPIAs are only mandated in high-risk data-processing operations, distinguishing these situations from non-high-risk personal data processing is not always straightforward. Furthermore, numerous provisions within various data and digital regulations could be subject to conformity assessments, thereby reducing compliance barriers to digital integration.

POLICY OPTION 5

Assignments of liability

Another practical approach to address the challenges faced by EU neighbouring countries in digital integration relates to liability issues. Regulations such as the GDPR, the AI Act and the Data Act assign responsibilities and liabilities to specific categories of actors. While these actors may play different roles in complex cross-border data operations, the issues that arise in data operations involving neighbouring countries are often simpler and associated more with uncertainties related to legal risks. The lack of formal recognition or agreements that facilitate cooperation between supervisory institutions can lead to blurred lines regarding responsibility and liability. This is a common issue in many cross-border data relationships.

While a firm operating in the EU market cannot absolve itself of liability for its data and data-processing activities, it could be advantageous for digital integration with neighbouring countries if EU firms could assume a greater share of liability for operations that involve data storage and processing by a third party in a third country. Although some degree of flexibility already exists in this regard, clarifying the operation of data regulations and making them more explicit, along with simplifying the process for defining liability within EU regulations, would be beneficial.

5. Concluding remarks

The EU's digital regulations, including the GDPR, create barriers that hinder its neighbouring countries from deepening their market engagement and exporting digital services to the EU. To mitigate these challenges, the EU should consider facilitating exports from these countries. This could involve revising and enhancing existing bilateral agreements and extending digital partnerships that are tailored to the specific needs of each neighbouring country. A key strategy could involve expanding adequacy and other mutual recognition mechanisms, thereby providing more integrated approaches for closer EU-neighbourhood collaboration. Another potential measure is to allow companies in partner countries to utilise EU supervisory bodies for regulatory compliance, effectively "lending" institutional authority. Additionally, the EU could introduce mechanisms enabling firms in other countries to self-declare compliance, thus reducing regulatory burdens. Finally, to further mitigate negative impacts, the EU could support its own firms by developing mechanisms that reduce liability risks when they engage in data operations within neighbouring jurisdictions.

The European Union positions itself as a pioneer in the evolving global landscape of data regulations, asserting that its policies will set a precedent for similar regulations in other major digital markets worldwide. This viewpoint has some validity, as seen through the widespread adoption of the EU's data privacy regulation, the GDPR, by various countries. Other EU data and processing regulations have also been embraced to varying degrees internationally. However, it's important to exercise caution in overextending this argument. For instance, while the EU's proposed AI regulation wields influence, other countries are advancing their own approaches, often diverging from the EU model. To minimise frictions with neighbouring countries, the EU must critically evaluate its regulatory strategy. A proactive approach, aimed at reducing integration barriers and smoothing access to the EU market for these countries, is essential.

Due to its substantial economic influence and interconnectedness, the EU is well-positioned as an influential geoeconomic entity, particularly within its immediate geographic sphere. However, recent and ongoing EU digital policies, such as the GDPR and the AI Act, have introduced complexities for its neighbouring countries that potentially push them away. Such policies not only risk alienating these countries but also diminishing their interest in economic and political integration with Europe. To counteract this, the EU should implement the mitigating policy measures discussed in this policy brief. These measures should be carefully tailored to address the unique circumstances of each neighbouring country to ensure they remain closely aligned with Europe.

Epilogue

This paper is the second in a series, following paper "The Carbon Border Adjustment Mechanism (CBAM) and Its Border Effects: How Can Europe Become a Better Neighbour?". It is part of the Bertelsmann Stiftung's project "Sovereign Europe: Strategic Management of Global Interdependence," under the Europe Programme. The series aims to offer a detailed perspective on the impact of the "Brussels Effect" on the European Union's (EU) neighbouring regions during a period marked by escalating geopolitical tensions. The focus of the paper series is on assessing the costs associated with the extraterritorial influence of EU internal market regulations on neighbouring areas engaged in trade with the EU. The regions analysed include the Western Balkans (Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia, Kosovo), Turkey, the Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine), and the Southern Neighbourhood (Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestine, Syria, Tunisia).

A central aspect of this research is proposing methods to mitigate the regulatory burden on these neighbouring regions. This enquiry is crucial as the EU seeks to maintain its regional influence amidst growing competition, notably from China. This work extends the study "Keeping friends closer: Why the EU should address new geoeconomic realities and get its neighbours back in the fold" concerning the EU's economic relationships with its neighbours, covering various domains like trade in goods and services, finance, technology, knowledge exchange, infrastructure, and labour mobility. Notably, the foundational study on interconnectivity was recognised by Foreign Affairs as one of the top ten books of 2023.

This analytical venture is conducted in partnership with the European Centre for International Political Economy (ECIPE), highlighting our commitment to providing insightful and actionable policy recommendations.

ANNEX 1
Overview of recent EU digital market regulations

General Data Protection Regulation
This section provides a more detailed overview of data protection rights, the role of the controller and processor as well as the fines and penalties associated with the GDPR.

Data protection rights
The GDPR grants data subjects powerful rights regarding how companies retain and process their personal data. These rights include:[26]

1. Right to be Informed (Article 13 and Article 14): Individuals have the right to receive information about the collection and utilisation of their personal data, imposing various information responsibilities on the controller.

2. Right of Access (Article 15): Individuals are entitled to confirmation of their data being processed, access to their personal data, and additional supplementary information, aligning closely with the details included in a typical privacy notice.

3. Right to Rectification (Article 16): Individuals have the right to correct inaccurate or incomplete personal data.

4. Right To Erasure (Article 17): Individuals have the right to request the deletion or removal of their personal data when there is no compelling reason for its continued processing.

5. Right To Restriction of Processing (Article 18): Individuals can "block" or suppress the processing of their personal data.

6. Right To Data Portability (Article 20): Individuals can obtain and utilise their personal data across various services for their own purposes. This right facilitates the smooth and secure movement, copying or transfer of personal data from one IT environment to another without compromising usability.

7. Right To Object Processing (Article 21): Individuals have the right to object to processing based on legitimate interests or the execution of a task in the public interest/exercise of official authority; direct marketing; and processing for scientific/historical research or statistical purposes.

8. Rights in relation to automated decision making and profiling (Article 22): Individuals have the right to avoid being subjected to decisions that have significant legal effects or similarly impactful outcomes solely based on automated processing, including profiling.

Under the GDPR, entities handling personal data are categorised as either data controllers or data processors. Understanding their roles is essential to maintaining GDPR compliance.

The role of the controller and processor (Article 4) [27, 28]
A data controller, whether a company, legal entity or person, is the entity responsible for determining the objectives and methods of data processing. In this role as the primary decision-maker, the data controller exercises authority and control over the rationale and objectives behind data collection, as well as the methods and processes involved in data processing. They are obligated to comply with all data protection principles, which include fairness, legality and transparency when processing personal data, as outlined in Article 24 of the GDPR. Furthermore, Article 26(1) of the GDPR grants data controllers the authority define the purposes and methods of data processing either independently or collaboratively with another party, acting as joint data controllers.[29]

In turn, a data processor is an individual or entity tasked with handling personal data on behalf of the data controller. Both the data controller and the data processor are directly responsible for privacy compliance under the GDPR. When conducting data-processing activities as instructed by the data controller, the data processor is required to adopt suitable organisational and technical measures in accordance with the GDPR's specified guidelines, as described in Article 28 of the GDPR). Additionally a data processor is obligated to process personal data strictly in line with the instructions provided by the data controller, except when compelled by legal requirements, as articulated in Article 29 of the GDPR.

26 ICO (nd). Overview of the General Data Protection Regulation (GDPR). https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf
27 GDPR data controllers and data processors. https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and processors/#:~:text=According%20to%20Article%2029%20of,data%20controllers%20and%20data%20processors
28 Ibid
29 European Commission. What is a data controller or a data processor? https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en
An example provided by the European Commission: Take a company which offers babysitting services via an online platform. At the same time, the company has another contract which will allow to offer value added services. These services include the possibility for parents not only to choose the babysitter but also rent games/movies which the babysitter can bring. As such, both the companies are involved in technical set-up of the website. Both companies have decided to use the platform for both service and will very often share client's names. As such the two companies become joint controllers, because they have agreed to offer the possibility of combined services through a common platform.

Individual users have the right to file compensation claims and seek damages from both data controllers and data processors. If a data processor deviates from the instructions of the data controller, they can be held responsible for any data breaches.

Fines and penalties: Article 83(5)[30]

Any violation of data subject rights can lead to the most severe penalties under the GDPR, which can amount to €20 million or 4% of the total global turnover from the previous fiscal year, depending on which is greater. Even lesser violations, as outlined in Article 83(4) of the GDPR, can result in fines of up to €10 million or, for an 'undertaking,' up to 2% of its entire global turnover from the preceding fiscal year, again depending on which is higher.[31]

Furthermore, each member state is required to establish regulations governing penalties for GDPR violations that go beyond those outlined in Article 83. These regulations may encompass criminal penalties or repercussions for breaches of national rules under the GDPR.

The Digital Markets Act

The DMA is a recently introduced regulation, adopted in the autumn of 2022, that establishes rules for, in particular, very large online platforms referred to as "gatekeepers". Its primary objective is to enhance competition in the digital space by creating a more accessible environment for new and smaller online platforms to enter and thrive in the market. The act builds on the principles of competition policy economics and incorporates decades-long expert and academic discussions regarding both ex ante and ex post competition policies. It addresses the challenges posed by rapidly evolving sectors heavily influenced by the dynamics of two-sided network markets. However, it is important to recognise that the motivation behind the DMA extends beyond the realm of competition policy. It also reflects broader political considerations and a general desire to align the behaviour of major platforms with the EU's overarching goals for these platforms and the markets they operate in.

The DMA aims to promote competition, contestability and fairness in the digital landscape. While the regulation references objectives such as consumer protection and innovation, its core premise lies in the belief that gatekeepers possess entrenched and enduring market positions that provide them significant market power and the ability to engage in practices that stifle competition and fairness. The DMA operates on the assumption that market developments in some digital services over the past decade have conferred excessive market power upon large platforms,and that traditional competition policy measures are insufficient to address the resulting market power's uses and abuses. Consequently, the DMA serves as a targeted regulation with ambitions to reshape sector-specific market regulations.

The Digital Services Act

The Regulation on a Single Market for Digital Services, also known as the Digital Services Act (DSA),[32] aims to enhance accountability among online platforms and intermediaries. It achieves this by establishing greater transparency and user safety through various means, such as implementing rules related to transparency obligations, due diligence requirements, and liability rules concerning third-party content. The DSA was approved by both the European Parliament and Council on October 19, 2022, and it will become directly applicable as of 1 January 2024, which is fifteen months after its adoption. While the primary goal of the regulation is to ensure the proper functioning of the single market and cross-border digital services, its scope clearly extends beyond this specific objective. The DSA governs the obligations of digital platforms that act as intermediaries in connecting consumers with goods, services and digital content. One notable area of focus within the DSA pertains to the regulation of social media content.

The DSA builds on the e-Commerce Directive of 2000, which served as the primary policy for regulating intermediary liability in the EU. It adapts the liability regime to the modern digital communication landscape, taking into account two decades of rapid growth in the platform and platform services sectors. However, the motivation for the DSA also stems from the growing size and market influence of digital service providers and platforms. Consequently, these entities will now be subject to more stringent behavioural rules that encompass aspects such as illegal content, platform access, and the traceability of platform transactions. Additionally, the DSA is aimed at enhancing online regulations concerning freedom of speech and the overall safety of any online presence.

The Data Act

In February 2020, the European Commission proposed new legislation aimed at regulating the use and accessibility of data within the EU, known as the Data Act. This legislation is part of the EU's Data Strategy, which seeks to increase the availability of data for commerce and society, while granting consumers and companies more control over the handling of their data. The Data Act encompasses several policy objectives set forth by the Commission, including the promotion of fairness in Europe's digital single mar-

30 Intersoft consulting. GDPR Fines / Penalties. https://gdpr-info.eu/issues/fines-penalties/
31 The term "undertaking" aligns with Art. 101 and 102 of the Treaty on the Functioning of the European Union (TFEU), encompassing not only individual companies but also multiple natural persons or corporate entities. This allows a group to be considered a single undertaking, using its total global annual turnover to determine fines for GDPR violations by any of its companies.
32 European Commission (2022). Regulation 2002/2065 on a Single Market for Digital Services. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

ket, the stimulation of competition in data markets, the facilitation of data-driven innovation, and the enhancement of data accessibility for all. More specifically – and in line with the European communication on a strategy – the Data Act aims to foster data-sharing between businesses and government authorities (B2G) for the common good, as well as support data-sharing between businesses (B2B). It also aims to revise the EU's existing intellectual property framework for databases to further enhance data accessibility and use.

With the Data Act, the Commission intends to address potential imbalances in bargaining power between data holders and those seeking access their data, which can lead to unfair data licencing terms or the outright refusal to grant data access. The Data Act also aims to address the issue of inadequate private contracts governing access to and use of non-personal data generated in industrial contexts. Such inadequacies have the potential to hinder competition in specific markets and leave untapped the innovative potential associated with reusing this data. The legislation also seeks to clarify the legal framework surrounding the application of the Database Directive to machine-generated data and data generated by IoT devices.

To mitigate the problems identified by the Commission, the proposed Data Act includes a series of rules governing data access and use in both B2B and B2G contexts. These rules encompass user control and the right to share user-generated data, the implementation of a fairness test in B2B interactions, the establishment of licencing criteria based on fair, reasonable and non-discriminatory (FRAND) market rates, and the introduction of new rights for the public sector to access privately held data for public interest purposes.

ANNEX 2
Characteristics and patterns of EU neighbourhood countries regarding digital services trade

Technological Hubs: Israel and Türkiye

Israel distinguishes itself as a leader in telecommunications, computer technology and information services, boasting an impressive export value of $2739 million. Conversely, Türkiye presents a diverse digital landscape with substantial contributions across various sectors, including insurance, financial services, and intellectual property charges.

Ukraine and Egypt: sector specialists

Ukraine's notable emphasis on information services, amounting to $1197 million, underscores its specialisation in this sector. Before Russia's full-scale war of aggression in 2022, Ukraine had been on the frontier of digital transformation, ranking as one of the world's largest exporters of information technology and services. Its robust pre-war digital ecosystem attracted major corporations such as Microsoft, Boeing, Google and Ericsson, which established subsidiaries in the country. At the same time, Ukraine saw the emergence of more than 4,000 local companies and the growth of globally recognised start-ups like Grammarly and GitLab.[33] In recent years, Ukraine has continued to specialise in strengthening and upskilling its workforce in areas such as cloud computing, AI and big data.[34] Despite the massive impact of the war on trade in services, Ukraine has managed to maintain its trade activity, with accounting for 26.7% of GDP in 2022.[35]

Likewise, Egypt has witnessed significant growth and specialisation in trade across telecommunications, computer technology, information services, insurance, financial services and other business-related domains. The information and communications technology (ICT) sector has become a pivotal driver of the country's economy, comprising 5% of the country's total GDP in recent years.[36] In an effort to expedite the process of digital transformation, Egypt is implementing various strategies that include training programmes and upskilling initiatives aimed at equipping the country's young workforce with essential ICT competencies. Initiatives such as "Our Future is Digital" or the "Our Digital Opportunity", tailored for SMEs, exemplify Egypt's commitment to advancing its digital landscape.[37]

33 Nair, S. (2022). Prominent tech companies that originated from Ukraine. https://analyticsindiamag.com/prominent-tech-companies-that-originated-from-ukraine/#:~:text=The%20Ukrainian%20IT%20industry%20consists%20of%20over%204%2C000,established%20their%20R%26D%20sector%20in%20Ukraine.%20THE%20BELAMY

34 Bandura, R. and Staguhn, J. (2023). Digital Will Drive Ukraine's Modernization. CSIS. https://www.csis.org/analysis/digital-will-drive-ukraines-modernization

35 One explanation is that the EU, for its part, has started drafting and implementing policies geared toward reconstruction efforts. The European Union has initiated several agreements to support Ukraine's digital development, such as the agreement to "Associate Ukraine to the Digital Europe Programme". Such initiatives are designed to support the rebuilding efforts in the digital sector for private companies as well as civil organisations and government agencies. https://digital-strategy.ec.europa.eu/en/policies/support-ukraine; https://tradingeconomics.com/ukraine/trade-in-services-percent-of-gdp-wb-data.html

36 International Trade Organization (2022). Information and Communications Technology, and Digital Economy. Egypt: Country Commercial Guide. www.trade.gov/country-commercial-guides/egypt-information-and-communications-technology-and-digital-economy

37 Ibid

Diverse portfolios: Morocco and Serbia

Morocco's role in the digital landscape is becoming increasingly prominent. A prime example of this is Morocco's well-established mobile market, which stands as one of the most mature in the region. The number of mobile subscribers surpasses the country's estimated population of 36 million, reaching an impressive 49.42 million subscribers. Morocco is actively striving to position itself as a leading technology hub in North Africa. To achieve this goal, the country is taking substantial measures to attract foreign direct investment in telecommunications and 5G infrastructure. There's also a concerted effort to promote industries that indirectly support the ICT sector, with nearshoring in Morocco having already created nearly 110,000 jobs.[38] Morocco digital services exports demonstrate diversity, with a focus on telecommunications, computer technology and information services totalling $614 million. The country's prospects depend largely on the development of digital businesses and strategic investments, both of which are key drivers of development.

Digital transformation has significantly impacted Serbia's economy, particularly in the domains of telecommunications and intellectual property. Despite considerable efforts to integrate into other digital markets, Serbia faces structural barriers hindering its full integration with regional and world services markets. For instance, Serbian businesses, including larger companies, have struggled to adopt digital and cloud technologies due to inadequate digital infrastructure,[39] with some regions suffering from poor connectivity and unreliable electricity supply.[40] The European Union has played a pivotal role in Serbia's economic and digital transformation as an external partner. Over recent years, the European Union has implemented various policies aimed at advancing digital capabilities in the Western Balkans, exemplified by initiatives like the "Digital Agenda for the Western Balkans" which places a strong emphasis on improving digital infrastructure and skills.[41]

Emerging players: Albania, Algeria, Bosnia, Kosovo and North Macedonia

Several countries are emerging as potential partners for the EU's digital trade initiatives. Albania, Bosnia, Kosovo and North Macedonia have grown their trade across various digital sectors. However, there remains significant untapped potential for further expansion that is contingent on the reduction of impediments and restrictions. Notably, Algeria, Egypt and Tunisia rank among the EU's neighbouring countries with the highest number of trade restrictions in services.[42] These barriers, encompasing diverse forms of non-tariff barriers, range from poor infrastructure to divergent domestic regulatory policies and market access limitations, all of which hinder investment and economic development.

Consider Algeria as an illuswrative case. The share of digital services in Algeria's trade is relatively modest and is partly attributable to its significant reliance on oil exports. Trade in services constitutes only 8.5% of GDP, in contrast to the Middle East and North Africa,s 20% in 2017.[43, 44] Recognising the need to diversify its economy for improved living standards, Algeria will need to diversify its economy to lift living standards, has set its sights on the IT sector as a key element of its export diversification strategy.[45] The Algerian government has demonstrated its commitment to bridging the digital services gap with other countries, with substantial investments exceeding $3.7 billion directed towards strengthening its ICT infrastructure from 2010 to 2019. Today, IT investments account for between 10% and 15% of all professional investments, presenting significant opportunities for countries engaged in the export of software, hardware and machinery.[46] Moreover, during the period spanning 2015 to 2019, Algeria engaged in significant imports of ICT equipment, amounting $22 billion.[47] This effort underscores the country's determination to catch up with other countries in the digital domain.[48]

38 Tobi, Y. (2023). E-commerce and the Digital Economy in Morocco, A Factor of Social Inclusivity and Employment: Context, Approach and Limits. www.euromesco.net/wp-content/uploads/2023/02/EuroMeSCo-Paper-58.pdf
39 Ibid
40 Mdrović, P. (2023). The role of digitalization in transforming Western Balkan societies. www.oegfe.at/policy-briefs/the-role-of-digitalisation-in-transforming-western-balkan-societies/?lang=en
41 European Commission (2018). European Commission launches Digital Agenda for the Western Balkans. https://ec.europa.eu/commission/presscorner/detail/es/IP_18_4242
42 Lejarra, I. (2023). Tricks of the trade: Strengthening EU-African cooperation on trade in services. https://ecfr.eu/publication/tricks-of-the-trade-strengthening-eu-african-cooperation-on-trade-in-services/
43 United Nations Statistics Division, UN COMTRADE. International Merchandise Trade Statistics. http://comtrade.un.org/
44 It is important to note that although Algeria has trade agreements in place with other countries, it is not a member of the WTO. Its oil-centred dependency, along with its exclusion from multilateral agreements such as GATT or GATS, bears implications for its competitive stance, despite being the second-largest economy in North Africa behind Egypt.
45 International Trade Organization (2022). Information and Communications Technology, and Digital Economy- Algeria: country commercial guides. www.trade.gov/country-commercial-guides/algeria-information-communications-technologies
46 Ibid
47 International Trade Administration & U.S. Department of Commerce. (2023, January 31). Algeria Information & Communications Technologies. https://www.trade.gov/country-commercial-guides/algeria-information-communications-technologies
48 In addition, bilateral business associations, including France's Business France Algérie and CCI France Algérie, play a pivotal role in fostering Algeria's trade with key partners, particularly France. Financial services are the main source of Algerian-French collaborations, especially through the presence of Société Générale and BNP Paribas, and transport with companies such as Air France.

ANNEX 3

Overview of agreements and relevant data-related provisions between the EU and its individual neighbourhood countries

[+] Is part of the European neighbourhood policy.
** Has applied for EU membership.

Country	Type of Agreement	Year	Data Provision Background
Israel[+]	▪ EU-Israel relations are governed by an Association Agreement in force since 2000. ▪ Adequacy decision on data protection: Israel is one of the few countries, and the only one in the EU's neighbourhood, to have been granted adequacy by the EU Commission.	2011	▪ Israel's data protection standards align with EU Directive 95/46/EC, signifying that Israel offers a sufficient level of personal data protection as per its legal requirements.[49] ▪ However, there are concerns that the EU could withdraw Israel's adequacy status. Recent proposals aimed at reforming Israel's justice system, which have sparked massive protests, are facing criticism due to concerns about the independence of the Supreme Court. While negotiations for an updated adequacy decision with the EU are still ongoing, they are currently on hold until Israel's legal and political situation becomes more stable and certain.[50]
Western Balkans and Türkiye			
Albania and North Macedonia[51] **	1. Stabilisation and Association agreement.[52, 53] 2. EU Membership process: ▪ Albania applied for EU membership on 28 April 2009. In 2014 the Commission recommended granting Albania the status of candidate for EU membership. ▪ Macedonia applied for EU membership in 2004. It was granted candidate status in 2005.	2009	▪ The legal basis for the relationship between the EU and Albania is the Stabilisation and Association Agreement, a key step in the process towards EU membership. Within this agreement, there are two articles relevant to data handling: Article 10, which permits the exchange of personal data under the condition that the receiving country provides equivalent safeguards as the sending country, and Article 79, which specifically provides for the protection of personal data. ▪ In the case of North Macedonia, the treatment of personal data is stated in Protocol 5 to the Stabilisation and Association agreement under Article 10,[54] which also mimics Article 10 of the EU-Albania agreement. ▪ In 2008, the Republic of Albania implemented the Data Protection Law.[55] This legislation has been amended twice. First in 2016 to bring it into line with the EU's Regulation 2016/679, and in 2016 to harmonise it with the GDPR. Similarly, in 2020, North Macedonia: passed a new "Law On Personal Data Protection that will align its domestic privacy legislation with the GDPR.
BiH **	1. Stabilisation and Association Agreement.[55] ▪ The SAA between the EU and BiH was negotiated and signed in 2008, but did not enter into force until 2015. This delay was due to BiH's failure to comply with a human rights ruling issued by the European Court of Justice. 2. EU Membership process: ▪ The European Council granted candidacy country status to BiH in December 2022.[56]	2015	▪ Bosnia and Herzegovina is required to harmonise its personal data protection law with Community law and other relevant European and international legislation. In addition, BiH must establish independent supervisory bodies to ensure the enforcement of its national personal data protection regulations, as stated in Article 79. ▪ Under the SAA, the exchange of personal data is permissible only if the receiving party commits to safeguarding that data in a manner equivalent to the standards applicable in the party providing the data, as outlined in Article 10.2 of Protocol 5.
Montenegro **	1. Stabilisation and Association Agreement.[57] 2. EU Membership process: ▪ Applied for EU membership in December 2008 and granted candidate status in December 2010. Accession negotiations began in June 2012.	2010	▪ Currently, Montenegro's personal data protection is governed by the Law on Protection of Personal Data (LPPI), which was last amended in 2017, a year before the GDPR came into effect.[58] As Montenegro seeks EU membership, it will eventually need to align its domestic legislation with the GDPR. An intriguing observation is that a consultancy group named Cervaluate offers "GDPR certification" for businesses, with varying levels of certification to ensure GDPR compliance.[59] This suggests that compliance with EU law may not necessarily wait for Montenegro's domestic law amendments. It is highly likely that businesses recognise the importance of EU law compliance and may proactively adapt their systems even before domestic legislation, mirroring EU regulations, is enacted

49 EU Directive 95/46/EC of the European Parliament and the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046
50 European Parliament E-001478/2023. www.europarl.europa.eu/doceo/document/E-9-2023-001478_EN.html
51 Note: Accession negotiations with Albania and Macedonia are treated jointly because of a shared positive recommendation from the Commission.
52 Official Journal from the European Union (2009). Stabilisation and Association Agreement between the European Communities and their Member States with the Republic of Albania. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2009.107.01.0165.01.ENG&toc=OJ%3AL%3A2009%3A107%3ATOC#L_2009107EN.01016601
53 Official Journal from the European Union (2004). Stabilisation and Association Agreement between the European Communities and their Member States and the former Yugoslav Republic of Macedonia. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A22004A0320%2803%29
54 Official Journal from the European Union (2004). Protocol 5 of the Stabilisation and Association Agreement between the European Communities and their Member States and the former Yugoslav Republic of Macedonia. https://eur-lex.europa.eu/resource.html?uri=cellar:3ce414a8-cc67-4879-a8cc-17b9c4745465.0007.02/DOC_6&format=PDF
55 Official Journal from the European Union (2015). Stabilization and Association Agreement between the European Communities and their Member States, of the one part, and Bosnia and Herzegovina, of the other part. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A22015A0630%2801%29
56 European Parliament (n.d.). The Western Balkans Fact Sheet. www.europarl.europa.eu/factsheets/en/sheet/168/the-western-balkans
57 Official Journal of the European Union (2010). Stabilization and Association Agreement between the European Communities and their Member states, and the Republic of Montenegro. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2010.108.01.0001.01.ENG&toc=OJ%3AL%3A2010%3A108%3ATOC
58 Chambers and Partners (2022). Montenegro's Personal Data Protection and the EU's GDPR. https://chambers.com/articles/montenegros-personal-data-protection-lppi-and-the-eus-gdpr
59 Certvalue (n.d.). GDPR Certification in Montenegro. www.certvalue.com/gdpr-certification-in-montenegro/

Serbia **	1. Stabilisation and Association Agreement.[60] 2. EU Membership process: ▪ Applied for EU membership in December 2009 and granted candidate country status in March 2012.	2013	▪ To date, 22 out of 35 negotiating chapters have been initiated. The four chapters that constitute "Cluster Four," focusing on the green agenda and sustainable connectivity, were opened in December 2021 following a 2-year hiatus without any new chapters being introduced. ▪ In 2018, Serbia passed the Personal Data Protection Law, which closely aligns with the GDPR and features only minor differences. Despite this alignment, the Serbian business and legal environment's lack of readiness has led to challenges in effectively implementing the law.[61]
Kosovo **	1. Stabilisation and Association Agreement.[62] 2. EU Membership process: ▪ Kosovo's future integration with Serbia remains closely linked to the EU-facilitated high-level dialogue between Kosovo and Serbia that aims to the normalisation of their relations.	2016	▪ Following the normalisation of relations through the Brussels Agreement in 2013 between Belgrade and Pristina, the European Council decided to initiate negotiations on a SAA with Kosovo. This agreement came into effect in April 2016. ▪ Kosovo's personal data protection is regulated by the Law on Personal Data, which entered into force in February 2019. This law was drafted in conformity with the GDPR. ▪ Kosovo's implementation of a new data regime is facing many challenges.[63]
Türkiye **	1. Customs Union. 2. EU Membership process: ▪ In 1987, Türkiye applied for EU membership when the European Economic Community was in existence. In 1999, it became eligible to join the EU.	1995	▪ The legal framework governing the relationship between the EU and Türkiye is the Customs Union, which encompasses all industrial goods but does not cover agriculture (except for processed agricultural products), services or public procurement. In 2016, the Commission proposed modernising the agreement to include services, but progress has been halted as the Council has not yet adopted the negotiating directives. ▪ Türkiye's Data Protection regime known as KVKK,[64] was designed to align Turkish legislation with the EU's Directive 95/46/EC, which governed data in the EU before the introduction of the GDPR.
Eastern Partnership			
Armenia *	1. A Comprehensive and Enhanced Partnership Agreement (CEPA)[65] was signed in November 2017 that fully entered into force in March 2021. CEPA replaced the previous Partnership and Cooperation Agreement of 1999. Until January 2022, Armenia benefited from the EU's GSP+ scheme, which offers preferential access to the EU market.	2021	▪ The parties involved in the CEPA agreed to cooperate to ensure a high level of protection, as outlined in Article 13. This protection is aimed at being in harmony with the development of electronic commerce and ensuring the trust of electronic commerce users (as stated in Article 193.2) and data processing for financial services (as per Article 185). Furthermore, the CEPA is compatible with the TRIPS agreement, as indicated in Article 249). ▪ While the GDPR does not apply in Armenia, the country has adjusted its domestic legislation to mirror the EU's legal instrument. Armenia's primary legal basis for data protection is the Law of Armenia on the Protection of Personal Data, and additionally, the country's Constitution safeguards the right to personal data protection.[66]
Azerbaijan *	1. Partnership and Cooperation Agreement.[67]	In force since 1999	▪ Personal data can only be exchanged when the receiving party commits to protect that data at a level equal to the standards applicable in the party providing the data. ▪ The responsibility for implementing this protocol lies with the central customs authorities of the Republic of Azerbaijan on one side and the relevant services of the Commission of the European Communities, and when necessary, the customs authorities of the member states on the other side. They are responsible for determining all practical measures and arrangements required for its application, while also considering the existing data protection regulations. They have the authority to suggest amendments to this protocol to the appropriate bodies if they deem it necessary.
Belarus *	N/A	N/A	▪ The Belarusian regime has formally suspended its participation in the Eastern Partnership policy, and it has suspended its participation in established structures such as the EU-Belarus Human Rights Dialogue and the EU-Belarus Coordination Group.

60 Official Journal of the European Union (2013). EU-Serbia Stabilisation and Association Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2013.278.01.0001.01.ENG&toc=OJ%3AL%3A2013%3A278%3ATOC
61 IAPP (2023). The state of Serbia's Personal Data Protection Law after two years. https://iapp.org/news/a/serbian-law-on-personal-data-protection-law-after-two-years-of-implementation-and-harmonization-with-gdpr/
62 Office Journal of the European Union (2016). Stabilisation and Association Agreement between the European Union and the European Energy Community and Kosovo. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22016A0316%2801%29
63 Zejnullah, N. (2020) Personal Data Protection in Kosovo, Three Years of Failure. https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl6&div=43&id=&page=
64 Personal Data Protection Authority (2016). Personal Data Protection La. www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law
65 Official Journal of the European Union (2018). Comprehensive and Enhanced Partnership Agreement between the European Union and the European Atomic Energy Community and the Republic of Armenia. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22018A0126(01)
66 Beglaryan, N. (2019). Data protection in Armenia: overview. www.dialog.am/storage/files/posts/posts_184625614492_2019_-_Global_Guide_-_TR_-_Data_protection_in_Armenia_-_overview.pdf
67 Official Journal of the European Union (1996). Partnership and Cooperation Agreement between the European Communities and their Member States and the Republic of Azerbaijan. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:21999A0917%2801%29

Georgia * ***	1. The EU- Georgia Association Agreement, which includes a DCFTA[68] entered into force in 2016. 2. EU Membership: ▪ Following Russia's full-scale war of aggression in Ukraine, Georgia, along with the Republic of Moldova, submitted its own application for candidate status in March 2022 under an accelerated procedure. However, Georgia was the only country (of these three) that was not granted candidacy status in June 2022.[69] Although Georgia has undertaken significant reforms in preparation for EU membership, the political climate in recent years has hampered progress. Factors such as political polarisation, increased corruption and oligarchic influences have contributed to a slowdown in democratic transformation.[70] ▪ While a majority of the Georgianpopulation supports its path toward EU integration, the country has seen a significant rise in political and economic ties with Russia since the war in Ukraine began.[71] Although the EU Commission has provided key recommendations to the Georgian government for achieving candidate status, the recent thaw in relations with Russia[72] makes it unlikely that Georgia will have a swift path to EU candidacy.[73]	2016	▪ The EU-Georgia Association Agreement includes provisions for the parties to cooperate in maintaining a high level of personal data protection in alignment with EU provisions (Article 14 and Annex II). They also agree to ensure adequate safeguards for the protection of privacy and fundamental rights, and freedom of individuals with regard to the transfer of personal data (Article 118). Each party guarantees the confidentiality of electronic communications and related traffic data (Article 111). ▪ Within the EU-Georgia Association Agreement, both parties have agreed that the development of electronic commerce must adhere to international standards, as stated in Article 127.
Moldova **	1. Association Agreement74 and a DCFTA. 2. EU Membership: ▪ Following Russia's full-scale invasion of Ukraine, Moldova (along with Georgia) submitted its application for candidate status in March 2022 under an accelerated procedure. Moldova was granted candidate status in June 2022.[75]	2016	▪ Under the Association Agreement between the EU and Moldova, the parties commit to collaborating to maintain a high level of personal data protection in alignment with EU provisions (Article 13). They also agree to establish sufficient safeguards to protect individuals' privacy, fundamental rights, and freedom concerning the transfer of personal data (as outlined in Article 245). ▪ The parties agree that the development of electronic commerce should adhere to the highest international standards (as specified in Article 254) and seek to enhance the security of personal data and privacy in electronic communications (as stipulated in Article 99). They also agree that the cross-border supply of services should not be subject to customs duties (Article 254.2). ▪ As part of the implementation of the Association Agreement, the parties commit to providing legal protection in line with EU Directive 95/46/EC (GDPR) (Annex I to Title III). Moreover, personal data may only be exchanged when the receiving party ensures adequate protection as deemed by the party supplying the data, as outlined in Protocol III, Article 10. ▪ In 2021, Moldova amended its existing Law on Personal Data Protection to introduce new obligations, aligning this law with the EU's GDPR.[76]
Ukraine **	1. Deep and Comprehensive Association Agreement (DCFTA).[77] 2. EU Membership: ▪ Ukraine applied for EU membership in February 28, 2022, immediately following the Russian invasion of its territory. It was granted candidate status in June 2022.	2014	▪ Within the DCFTA between the EU and Ukraine, the parties agree to cooperating to maintain an adequate level of personal data protection in accordance with the highest standards (as articulated in Article 15). They ensure sufficient safeguards to protect the privacy, fundamental rights and freedom of individuals (as detailed in Article 129). The exchange of personal data is permissible only if the receiving party provides an adequate level of protection in accordance with these standards (as stated in Article 10 of Protocol III). Furthermore, the transmission of personal data may occur solely when it is necessary for the implementation of this agreement by the relevant authorities of Ukraine or the EU, as the case may be (Article 10, Annex XLIII to Title VI).

68 Official Journal of the European Union (2014). Association Agreement between the European Union and the Atomic Energy Community and their Member States and Georgia. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.261.01.0004.01.ENG
69 Stone, S. (2023). Reform and Resistance: Georgia's Path to EU candidacy. https://cepa.org/comprehensive-reports/reform-and-resistance-georgias-path-to-eu-candidacy/
70 Fix, L. and Kapp, C. (2023) The Dangers of Democratic deconsolidation in Georgia. www.cfr.org/article/dangers-democratic-backsliding-georgia
71 Ibid
72 Kramer, D. and Kelly, I. (2023). The nation of Georgia's democratic future is slipping away. https://thehill.com/opinion/international/3874004-the-nation-of-georgia-democratic-future-is-slipping-away/
73 European Commission (2022). Opinion on the EU membership application by Georgia. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_3800
74 Official Journal of the European Union (2014). Association Agreement between the European Union and the European Atomic Energy Community and their Member States and the Republic of Moldova. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22014A0830(01)&from=EN
75 European Commission (2022). Communication from the Commission to the European Parliament, the European Council and the Council. https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-06/Republic%20of%20Moldova%20Opinion%20and%20Annex.pdf
76 DataGuidance (2022). Moldova: Amendments to the law on personal data protection. www.dataguidance.com/opinion/moldova-amendments-law-personal-data-protection-%E2%80%93
77 Official Journal of the European Union (2014). Association Agreement between the European Union and their Member States and Ukraine. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22014A0529(01)

Southern Neighbourhood			
Algeria *	1. Association Agreement.[78] 2. European Neighbourhood Policy.	2005	▪ Personal data can only be exchanged when the contracting party receiving the data commits to protecting such data at a level equivalent to that applied by the contracting party providing the data (Article 10). Additionally, the parties pledge to implement suitable measures to ensure the protection of personal data in order to remove barriers to the free flow of such data between them (Article 45 Title IV). ▪ In the realm of intellectual, industrial and commercial property, the parties have agreed to ensure the effective implementation of various multilateral conventions in intellectual property rights, including the WIPO Copyright Treaty and the Trademark Law Treaty (as outlined in Annex 6). ▪ The EU and Algeria have adopted several "Partnership Priorities"[79] covering areas like trade and access to the European single market. There's no mention of cooperation in the exchange of data. ▪ Algeria passed its own law on personal data protection in 2018.[80] The 2020 Doing Business Report highlights that the passing of this law may contribute to improving the business environment, making it more conducive to the use of financial services.[81]
Egypt *	1. Association Agreement.[82] (The EU and Egypt began talks about the modernisation of the bilateral relationship with the pursual of a DCFTA.) 2. Partnership priorities.	2004	▪ The Association Agreement does not include specific provisions related to data. However, it can be inferred that this aspect might be addressed in the modernised agreement, as it is outlined in the partnership priorities.[83] The only provision related to data protection in the association agreement can be found in the partnership priorities: ▪ In the context of promoting good governance and a modern democratic state, particularly under the subsection titled "Stabilising the common neighbourhood and beyond" (Partners in Foreign Policy), the EU and Egypt commit to cooperating to ensure a high level of personal data protection in accordance with international data protection standards. ▪ In 2020, Egypt passed the Egyptian Law No. 151 on Data Protection, which incorporates some provisions of the GDPR. It distinguishes between two types of data: personal data and sensitive date. Similar to the GDPR, it prohibits the processing of personal data without the consent of the data subject and imposes penalties and sanctions for violations.[84]
Jordan *	1. Association Agreement.[85] 2. Partnership priorities.[86]	2002	▪ Personal data can only be exchanged when the receiving party commits to protecting such data in a manner equivalent to what is applicable in the form in which the information is provided by the supplying party (Article 9) ▪ The protection of personal data is part of the Partnership priorities. To ensure a high level of personal data protection, the EU will continue its efforts to align with EU and international data protection standards. Jordan is also encouraged to take practical measures to ensure the respect for privacy rights and personal data protection in both public and private sectors, including in law enforcement and criminal justice (Article 9) ▪ Currently, Jordan does not have a data protection law in place.[87]
Lebanon *	1. Association agreement.[88] 2. Agreement on additional liberalisation of trade in agricultural products.	2006	▪ There is regulatory cooperation concerning international services, which includes considerations related to data protection and privacy (Article 53). ▪ The exchange of personal data is only permissible if the receiving contracting party commits to protecting the data at a level equivalent to the one applied in the contracting party that is providing the data, as outlined in Protocol 5.
Libya *	N/A		▪ Libya does not have an association agreement or other contractual agreement with the EU, but the country is eligible for funding under the NDICI and other financial instruments.
Morocco *	1. Association agreement in force since 2000.[89] Negotiations on modernisation began in 2013, on hold since 2014.	2000	In the Association Agreement, there is only one provision related to the handling of personal data, specifically Article 10 concerning the obligation to maintain confidentiality (Protocol 5). However, an entire annex to the agreement addresses this matter in detail.

78 Council of the European Union (2017). Association Agreement between the European Union and the People's Democratic Republic of Algeria. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22005A1010(01)&qid=1691935860919
79 European Council (2017). The European Union and Algeria Adopt their Partnership Priorities. www.consilium.europa.eu/en/press/press-releases/2017/03/13/eu-algeria/
80 Data Protection Africa (2022) Argelia: Data Protection Fact Sheet. https://dataprotection.africa/algeria/#:~:text=Privacy%20enshrined%20in%20Constitution%3A%20Yes,DPA%20legislation%3A%20Law%20No
81 World Bank (2020) Doing Business: Economy Profile of Argelia. https://archive.doingbusiness.org/content/dam/doingBusiness/country/a/algeria/DZA.pdf
82 UNCTAD (2004). Association Agreement between the European Communities and the Arab Republic of Egypt. https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/2514/download
83 European Council (2022). Association Between the European Union and Egypt. https://data.consilium.europa.eu/doc/document/ST-2803-2022-ADD-1/en/pdf
84 International Trade Administration (2020) Egypt data protection. www.trade.gov/market-intelligence/egypt-data-protection#:~:text=The%20law%20follows%20some%20of,effective%20on%20October%2015%2C%202020
85 Official Journal of the European Communities (2002). Association between the European Communities and their Member States and the Hashemite Kingdom of Jordan. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22002A0515(02)&from=EN
86 European Council (2022). Annex to the Decision of the EU-Jordan Association Agreement. https://data.consilium.europa.eu/doc/document/ST-3304-2022-ADD-1/en/pdf
87 Accessnow (2023). Policy Brief: What's wrong with Jordan's data protection law and how to fix it. www.accessnow.org/publication/jordan-data-protection-law/
88 Official Journal of the European Union (2006). Euro-Mediterranean Agreement establishing an association between the European Community and its Member States and the Republic of Lebanon. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22006A0530%2801%29
89 Official Journal of the European Communities (2000). Euro-Mediterranean Agreement establishing an association agreement between the European Communities and their Member States, and the Kingdom of Morocco. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:22000A0318(01)

Palestine *	1. Interim Association Agreement on trade and cooperation between the European Community, of the one part, and the Palestine Liberation Organization for the benefit of the Palestinian Authority of the West Bank and the Gaza Strip.[90]	1997	▪ Although the Palestinian Authority is the entity that most closely represents a government, its influence among Palestinians has diminished in recent years. It is also important to note that it operates primarily in the West Bank, where it has control over certain areas (while sharing control in others with Israel). However, it is not the governing authority in the Gaza Strip.
Syria *	N/A		▪ In May 2011, the EU suspended all its bilateral cooperation with the Syrian government due to the escalating violence and unacceptable human rights situation. The EU has also adopted various restrictive measures in the form of sanctions.
Tunisia *	1. Association Agreement[91] in force since 1998, negotiations on a DCFTA began in 2015, on hold since 2019. Discussions on the DCFTA are covering a wide range of issues including agriculture, services and sustainable development.	1998	▪ The exchange of personal data is only allowed when the level of protection provided to individuals in the legislation of the contracting parties is equivalent (Article 10). ▪ Personal data must be acquired and processed in a fair and lawful manner, and it should be retained for specific and legitimate purposes (Annex to the Association Agreement).

90 WITS World Bank (1997). Euro-Mediterranean Interim Association Agreement on Trade and Cooperation Between the European Community and the Palestine Liberation Organization for the Benefit of the Palestinian Authority of the West Bank and the Gaza Strip. https://wits.worldbank.org/GPTAD/PDF/archive/EC-PLO.pdf

91 Official Journal of the European Communities (1998). Euro-Mediterranean Agreement establishing an association between the European Communities and their Member States and the Republic of Tunisia. https://eur-lex.europa.eu/resource.html?uri=cellar:d3eef257-9b3f-4adb-a4ed-941203546998.0008.02/DOC_4&format=PDF

January 2024

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256 | D-33311 Gütersloh
Phone +49 5241 81-0

www.bertelsmann-stiftung.de
https://globaleurope.eu

Responsible
Stefani Weiss

Authors
Fredrik Erixon
Philipp Lamprecht
Erik van der Marel
Elena Sisto
Renata Zilli

All authors are affiliated with ECIPE.

Editing
Barbara Serfozo, Berlin
Design
Ines Meyer, Gütersloh
Printing
Hans Gieselmann Druck und Medienhaus, Bielefeld
Cover
© ii-graphics - stock.adobe.com

DOI 10.11586/2024006