POLICY BRIEF

Comparative analysis EU-Chile modernized trade agreement on digital trade in the context of other recent digital trade agreements concluded by Chile.

Maria Paz Canales[1]

27TH JANUARY 2023.

In November, 2002 Chile and the European Union (EU) signed an Association Agreement (the updated Association Agreement) that entered into force on February 1, 2003. Chile was the first South American country to sign an association agreement with the European Union.[2]

In December 2022, Chile and the EU signed a modernization of their Association Agreement. One of the novelties of this update was the addition of a digital trade chapter.[3]

In this brief we summarily analyze the similarities and differences between the provisions in the digital trade chapter and other provisions in other trade agreements such as Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTTP)[4] and the Digital Economy Partnership Agreement (DEPA)[5], recently concluded by Chile that touch on similar matters of digital trade.

1. *Online Consumer Trust*

CTPP	*DEPA*	*EU-Chile (December 2022)*
Article 14.7: Online Consumer Protection	***Article 6.3: Online Consumer Protection*** *1. The Parties recognise the*	***Article 19.10 - Online consumer trust*** *1. Recognising the importance of*

[1] Global Policy Advisor at Derechos Digitales.
[2] See, for example: EU trade relations with Chile. Facts, figures and latest developments. Available at: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/chile_en
[3] European Commission. EU and Chile strengthen a comprehensive political and trade partnership. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7569.
[4] Available at: https://www.subrei.gob.cl/acuerdos-comerciales/acuerdo-transpacifico-tpp11.
[5] Available at: https://www.subrei.gob.cl/landings/depa.

1. The Parties recognise the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent and deceptive commercial activities as referred to in Article 16.6.2 (Consumer Protection) when they engage in electronic commerce. *2. Each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.*	*importance of transparent and effective measures to protect consumers from fraudulent, misleading or deceptive conduct when they engage in electronic commerce.* *2. The Parties recognise the importance of cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border electronic commerce in order to enhance consumer welfare.* *3. Each Party shall adopt or maintain laws or regulations to proscribe fraudulent, misleading or deceptive conduct that causes harm, or is likely to cause harm, to consumers engaged in online commercial activities. Such laws or regulations may include general contract or negligence law and may be civil or criminal in nature. "Fraudulent, misleading or deceptive conduct" includes:* *(a) making misrepresentations or false claims as to material qualities, price, suitability for purpose, quantity or origin of goods or services;* *(b) advertising goods or services for supply without intention to supply;* *(c) failing to deliver products or provide services to consumers after the consumers have been charged; or* *(d) charging or debiting consumers' financial, telephone or other accounts without authorisation.* *4. Each Party shall adopt or maintain laws or regulations that: (a) require, at the time of delivery, goods and services provided to be*	*enhancing consumer trust in digital trade, each Party shall adopt or maintain measures to ensure the effective protection of consumers engaging in electronic commerce transactions, including but not limited to measures that:* *a) proscribe fraudulent and deceptive commercial practices;* *b) require suppliers of goods and services to act in good faith and abide by fair commercial practices, including through the prohibition of charging consumers for unsolicited goods and services;* *c) require suppliers of goods or services to provide consumers with clear and thorough information regarding their identity and contact details[1], as well as regarding the goods or services, the transaction and the applicable consumer rights; and* *d) grant consumers access to redress to claim their rights, including a right to remedies in cases where goods or services are paid and not delivered or provided as agreed.* *2. The Parties recognise the importance of cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to electronic commerce in order to enhance consumer trust.* ***Article 19.11 - Unsolicited direct marketing communications*** *1. Each Party shall ensure that end-users are effectively protected against unsolicited direct marketing communications.* *2. Each Party shall adopt or maintain effective measures regarding unsolicited direct*

	of acceptable and satisfactory quality, consistent with the supplier's claims regarding the quality of the goods and services; and *(b) provide consumers with appropriate redress when they are not.* *5. Each Party shall make publicly available and easily accessible its consumer protection laws and regulations.* *6. The Parties recognise the importance of improving awareness of, and access to, policies and procedures related to consumer protection, including consumer redress mechanisms, including for consumers from one Party transacting with suppliers from another Party.* *7. The Parties shall promote, as appropriate and subject to the respective laws and regulations of each Party, cooperation on matters of mutual interest related to misleading and deceptive conduct, including in the enforcement of their consumer protection laws, with respect to online commercial activities.* *8. The Parties endeavour to explore the benefits of mechanisms, including alternative dispute resolution, to facilitate the resolution of claims relating to electronic commerce transactions.*	*marketing communications that:* *a) require suppliers of unsolicited direct marketing communications to ensure that recipients are able to prevent ongoing reception of those communications; or* *b) require the consent, as specified according to the laws and regulations of each Party, of recipients to receive direct marketing communications.* *3. Each Party shall ensure that direct marketing communications are clearly identifiable as such, clearly disclose on whose behalf they are made and contain the necessary information to enable end-users to request cessation free of charge and at any moment.*

In CPTPP the focus on the online consumer protection is linked to "*protect consumers from fraudulent and deceptive commercial activities*". Similarly, in DEPA the provision looks to shield consumers from "*fraudulent, misleading or deceptive conduct when they engage in electronic commerce*".

The provision in the updated Association Agreement the focus seems wider as it aims to enhance "*consumer trust in digital trade*" by ensuring "*effective protection of consumers*

engaging in electronic commerce transactions". In that sense, the provisions cover not only fraudulent, misleading or deceptive conducts as the previous trade agreements with provisions in this matter, but also advance to require good faith in commercial practices and in the provision of information to consumers. It also requires access to redress for consumers in cases in which goods or services are paid and not delivered or provided as agreed, expanding the protection provided in DEPA, that only focused on claims of quality of products and services.

The three analyzed agreements highlight the need for cooperation between consumer authorities in order to enhance consumer trust, but DEPA includes further references to exploring alternative dispute resolution to facilitate the resolution of claims.

2. Protection of personal data and privacy

CTPP	***DEPA***	***EU-Chile (December 2022):***
Article 14.8: Personal Information Protection[5] *1. The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce.* *2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.*[6] *3. Each Party shall endeavour to adopt non-discriminatory practices in protecting users of*	***Article 4.2: Personal Information Protection*** *1. The Parties recognise the economic and social benefits of protecting the personal information of participants in the digital economy and the importance of such protection in enhancing confidence in the digital economy and development of trade.* *2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce and digital trade. In the development of its legal framework for the protection of personal information, each Party shall take into account principles and guidelines of relevant international bodies.*[11]	***Article 19.5 - Protection of personal data and privacy*** *1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.* *2. Each Party may adopt and maintain the measures it deems appropriate to ensure the protection of personal data and privacy, including the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective measures.* *3. For greater certainty, the Investment Court System does not apply to the provisions in Articles 19.4 and 19.5.*

electronic commerce from personal information protection violations occurring within its jurisdiction. *4. Each Party should publish information on the personal information protections it provides to users of electronic commerce, including how:* *(a) individuals can pursue remedies; and* *(b) business can comply with any legal requirements.* *5. Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them.* *Footnote n. 5 Brunei Darussalam and Viet Nam are not required to apply this Article before the date on which that Party implements its legal framework that provides for the protection of personal data of the users of electronic commerce.* *Footnote n. 6 For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal*	*3. The Parties recognise that the principles underpinning a robust legal framework for the protection of personal information should include:* *(a) collection limitation;* *(b) data quality;* *(c) purpose specification;* *(d) use limitation;* *(e) security safeguards;* *(f) transparency;* *(g) individual participation; and* *(h) accountability.* *4. Each Party shall adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction.* *5. Each Party shall publish information on the personal information protections it provides to users of electronic commerce, including how:* *(a) individuals can pursue remedies; and* *(b) businesses can comply with any legal requirements.* *6. Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall pursue the development of mechanisms to promote compatibility and interoperability between their different regimes for protecting personal information. These mechanisms may include:* *(a) the recognition of regulatory outcomes, whether accorded autonomously or by*	

information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.	*mutual arrangement;* *(b) broader international frameworks;* *(c) where practicable, appropriate recognition of comparable protection afforded by their respective legal frameworks' national trustmark or certification frameworks; or* *(d) other avenues of transfer of personal information between the Parties.* *7. The Parties shall exchange information on how the mechanisms in paragraph 6 are applied in their respective jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility and interoperability between them.* *8. The Parties shall encourage adoption of data protection trustmarks by businesses that would help verify conformance to personal data protection standards and best practices.* *9. The Parties shall exchange information on and share experiences on the use of data protection trustmarks.* *10. The Parties shall endeavour to mutually recognise the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers while protecting personal information.* ***Footnote n.** 11. For greater certainty, a Party may comply with*	

	the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering data protection or privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to data protection or privacy.	

From a values perspective there is a huge difference between the updated Association Agreement that recognizes the protection of personal data and privacy is a fundamental right, compared to DEPA and CPTTP that focused on the economic value and social benefits of protecting the personal information of participants in the digital economy.

Beyond the principled approach the updated Association Agreement makes explicit the leeway of each party in adopting regulation to better protect personal data and privacy, and explicitly excludes this matter as one susceptible of dispute resolution mechanism. On the contrary, both CPTPP and DEPA focused on adopting non-discriminatory practices in protecting personal information.

3. Cross border data flows and data protection

CTPP	***DEPA***	***EU-Chile (December 2022)***
Article 14.11: Cross-Border Transfer of Information by Electronic Means *1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.* *2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.*	***Article 4.3: Cross-Border Transfer of Information by Electronic Means*** *The Parties affirm their level of commitments relating to cross-border transfer of information by electronic means, in particular, but not exclusively:* *1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.*	***Chapter II - Data flows and personal data protection*** ***Article 19.4 - Cross-border data flows: prohibition of data localisation*** *The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by:* *a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or*

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: *(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and* *(b) does not impose restrictions on transfers of information greater than are required to achieve the objective.*	*2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.* *3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:* *(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and* *(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective."*	*network elements that are certified or approved in the territory of the Party;* *b) requiring the localisation of data in the Party's territory for storage or processing;* *c) prohibiting storage or processing in the territory of the other Party;* *d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory.*

The three instruments in analysis promote the cross border data flows as a way to facilitate digital trade. In the case of the updated Association Agreement there is a focus on the prohibition of data localisation.

In the case of CPTTP and DEPA, they expressly recognize the possibility of making exceptions on the cross border data flow when it comes to achieving a legitimate public policy objective. That being said, the **article 19. 1 bis** of the updated Association Agreement recognize a "right to regulate" that allows each party to regulate within their territories to achieve legitimate policy objectives, including privacy and data protection.

4. Source code disclousure

CTPP	***EU-Chile (December 2022)***
Article 14.17: Source Code *1. No Party shall require the transfer of, or access*	***Article 19.12 - Prohibition of mandatory transfer of or access to source code***

to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory. *2. For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure.* *3. Nothing in this Article shall preclude:* *(a) the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts; or* *(b) a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement.* *4. This Article shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to safeguards against unauthorised disclosure under the law or practice of a Party.*	*1. No Party may require the transfer of, or access to, source code of software owned by a juridical or natural person of the other Party.* *2. For greater certainty:* *a) the general exception, security exception and prudential carve-out can apply to measures of a Party adopted or maintained in the context of a certification procedure;* *b) paragraph 1 does not apply to the voluntary transfer of or granting of access to source code on a commercial basis by a person of the other Party, for instance in the context of a public procurement transaction or a freely negotiated contract;* *c) nothing in paragraph 1 prevents a person of a Party from licencing its software on a free and open source basis.* *3. Nothing in this Article shall affect:* *a) requirements by a court, administrative tribunal or, by a competition authority to remedy a violation of competition laws;* *b) protection and enforcement of intellectual property rights; and* *c) the right of a Party to take measures in accordance with Article 21.3 [security and general exceptions of the Public Procurement Title].*

CPTTP prevents the mandatory code source disclosure as a condition for the import, distribution, sale or use of such software, or of products containing such software. But that prohibition is limited to mass-market software or products containing such software and does not include software used for critical infrastructure.

The updated Association Agreement places a general prohibition on source code disclosure even broader than CPTPP that can be limited only by a general exception, security exception, certification procedure or voluntary disclosure.

Conclusion

In this first analysis, we see that there are some important advances regarding the treatment of digital trade in the document signed by Chile and the European Union this December 2022. Here we briefly review the articles related to online consumer trust, data protection, cross-border data flows and source code disclosure. In the specific case of consumer law, although it is not a step towards guaranteeing rights for European consumers, it may mean a step towards improving the laws and institutional environment for consumer protection in the digital age in Chile. In other cases, such as the source code disclosure, the language used in other treaties signed by the European Union are more protective of rights, and this may have been due to the fact that the text was proposed some years ago, so that it did not capture the progress of the language most current of treaties signed by Europe with other countries. We understand that more research is needed to (i) foster the comparison between the treaties, and (ii) to inquire whether in practice it would have an impact on industries, national laws, and the protection of rights.