

- (b) prevent parties to an electronic transaction from being able to prove to judicial and administrative authorities that the use of electronic authentication or an electronic trust service in that transaction complies with the applicable legal requirements.

3. Notwithstanding paragraph 2, a Party may require that for a particular category of transactions, the method of electronic authentication or trust service is certified by an authority accredited in accordance with its law or meets certain performance standards which shall be objective, transparent and non-discriminatory and only relate to the specific characteristics of the category of transactions concerned.

Article DIGIT.12: Transfer of or access to source code

1. A Party shall not require the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party.

2. For greater certainty:

- (a) the general exceptions, security exceptions and prudential carve-out referred to in Article DIGIT.4 [Exceptions] apply to measures of a Party adopted or maintained in the context of a certification procedure; and
- (b) paragraph 1 of this Article does not apply to the voluntary transfer of, or granting of access to, source code on a commercial basis by a natural or legal person of the other Party, such as in the context of a public procurement transaction or a freely negotiated contract.

3. Nothing in this Article shall affect:

- (a) a requirement by a court or administrative tribunal, or a requirement by a competition authority pursuant to a Party's competition law to prevent or remedy a restriction or a distortion of competition;
- (b) a requirement by a regulatory body pursuant to a Party's laws or regulations related to the protection of public safety with regard to users online, subject to safeguards against unauthorised disclosure;
- (c) the protection and enforcement of intellectual property rights; and
- (d) the right of a Party to take measures in accordance with Article III of the GPA as incorporated by Article PPROC.2 [Incorporation of certain provisions of the GPA and covered procurement] of Title VI [Public procurement] of this Heading.

Article DIGIT.13 Online consumer trust

1. Recognising the importance of 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, including when they act through intermediary service suppliers, regarding their identity and contact details, the transaction concerned, including the main characteristics of the goods or services and the full price inclusive of all applicable charges, and the applicable consumer rights (in the case of intermediary service suppliers, this includes enabling the provision of such information by the supplier of goods or services); and
- (d) grant consumers access to redress for breaches of their rights, including a right to remedies if goods or services are paid for and are not delivered or provided as agreed.

2. The Parties recognise the importance of entrusting their consumer protection agencies or other relevant bodies with adequate enforcement powers and the importance of cooperation between these agencies in order to protect consumers and enhance online consumer trust.

Article DIGIT.14 Unsolicited direct marketing communications

1. Each Party shall ensure that users are effectively protected against unsolicited direct marketing communications.
2. Each Party shall ensure that direct marketing communications are not sent to users who are natural persons unless they have given their consent in accordance with each Party's laws to receiving such communications.
3. Notwithstanding paragraph 2, a Party shall allow natural or legal persons who have collected, in accordance with conditions laid down in the law of that Party, the contact details of a user in the context of the supply of goods or services, to send direct marketing communications to that user for their own similar goods or services.
4. 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 users to request cessation free of charge and at any moment.
5. Each Party shall provide users with access to redress against suppliers of direct marketing communications that do not comply with the measures adopted or maintained pursuant to paragraphs 1 to 4.

Article DIGIT.15 Open government data

1. The Parties recognise that facilitating public access to, and use of, government data contributes to stimulating economic and social development, competitiveness, productivity and innovation.
2. To the extent that a Party chooses to make government data accessible to the public, it shall endeavour to ensure, to the extent practicable, that the data:
 - (a) is in a format that allows it to be easily searched, retrieved, used, reused, and redistributed;
 - (b) is in a machine-readable and spatially-enabled format;
 - (c) contains descriptive metadata, which is as standard as possible;