2020 G20 Riyadh Summit Final Compliance Report

Prepared by

Kaylin Dawe, Jae Yoon Mary Noh and the G20 Research Group
University of Toronto
Toronto
and
Alexander Ignatov and the Center for International Institutions Research
Russian Presidential Academy of National Economy and Public Administration,
Moscow

From 23 November 2020 to 27 September 2021

10 November 2021 (updated from 28 October 2021)

Feedback, as always, is welcome and is kept anonymous.
We encourage readers to send comments to
G20@utoronto.ca

Contents

5. Digital Economy: Consumer Rights

"We support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security."

G20 Riyadh Leaders' Declaration

Assessment

	No Compliance	Partial Compliance	Full Compliance
Argentina			+1
Australia			+1
Brazil			+1
Canada			+1
China		0	
France			+1
Germany			+1
India		0	
Indonesia			+1
Italy			+1
Japan			+1
Korea			+1
Mexico			+1
Russia			+1
Saudi Arabia			+1
South Africa		0	
Turkey			+1
United Kingdom			+1
United States		0	
European Union			+1
Average	+0.80 (90%)		

Background

For the first time ever the G20 addressed the issues related to digital growth in 2015. During Turkey's presidency, the G20 members approved national adjusted growth strategies; several of them, including Germany's, indicated "investing in research …and expanding the "High Tech Strategy" as a key long-term task."[2075] Approving adjusted growth strategies focused on the wide use of digital technologies in various spheres was the first step towards more specific initiatives and commitments. At Antalya, G20 leaders committed to "bridge the digital divide" and also noted that "states have a special responsibility to promote security, stability, and economic ties with other nations" in information and communications and technology (ICT).[2076]

At Hangzhou in 2016, in the G20 Blueprint on Innovative Growth, for the first time G20 leaders addressed the issue of proliferation of the digital economy, which they defined the digital economy as "a broad range of economic activities that includes using digitized information and knowledge as the key factor of production, modern information networks as the important activity space, and the effective use of ICT as an important driver for efficiency-enhancing and economic structural

[2075] Adjusted Growth Strategy: Germany, RANEPA (Moscow) 8 July 2017. Access Date: 13 January 2021. https://www.ranepa.ru/images/media/g20/2015Antalya/Adjusted-Growth-Strategy-2015-Germany.pdf

[2076] G20 Leaders' Communique Antalya Summit 15 – 16 November 2015, RANEPA (Moscow) 16 November 2015. Access Date: 13 January 2021. https://www.ranepa.ru/images/media/g20/2015Antalya/000111117.pdf

optimization."[2077] The leaders pledged to "offer policy support for an open, and secure ICT environment, including recognizing the key role of adequate and effective protection and enforcement of intellectual property rights to the development of the digital economy" by means of "cultivating transparent digital economy policy-making" and "supporting the development and use of international standards."[2078] To facilitate "the G20 agenda on innovation, new industrial revolution and digital economy," G20 leaders decided to establish a designated task force supported by the Organisation for Economic Co-operation and Development (OECD).[2079]

At Hamburg in 2017, the G20 addressed the issue of digital skills promotion. The #eSkills4Girls Initiative touched on the issue within broader context of development and gender policy.[2080] To facilitate implementing commitments on digital growth, the Digital Economy Task Force (DETF) was established following the decision made in Hangzhou in 2016.[2081] The leaders concluded with commitments aimed at harnessing digitalization and digital growth such as a pledge to promote digital literacy and digital skills, ensure effective competition to foster investment and innovation, promote effective cooperation of all stakeholders and encourage the development and use of market and industry-led international standards for digitized production, products and services.[2082]

During Argentina's G20 presidency in 2018, the DETF presented political tools for digital growth including the G20 Digital Governance Principles, recommendation for measuring the digital economy, gender equality in digital sphere and digital infrastructure development.[2083] At Buenos Aires, the G20 leaders pledged to "promote measures to boost micro, small and medium enterprises and entrepreneurs, bridge the digital gender divide and further digital inclusion, support consumer protection, and improve digital government, digital infrastructure and measurement of the digital economy."[2084]

Japan's G20 presidency in 2019 greatly expanded the G20 digital agenda. In Osaka, the G20 leaders presented the Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism, which tackled cyber security.[2085] In addition, the Osaka Declaration on Digital Economy was adopted in which most G20 members (with exception of India, South Africa and Indonesia) declared the launch of the "Osaka track" to promote discussions on "trade-related aspects of electronic commerce at the [World Trade Organization]."[2086]

[2077] G20 Blueprint on Innovative Growth, G20 Information Centre (Toronto) 5 September 2016. Access Date: 13 January 2021. http://www.g20.utoronto.ca/2016/160905-blueprint.html
[2078] G20 Blueprint on Innovative Growth, G20 Information Centre (Toronto) 5 September 2016. Access Date: 13 January 2021. http://www.g20.utoronto.ca/2016/160905-blueprint.html
[2079] G20 Leaders' Communique: Hangzhou Summit, G20 Information Centre (Toronto) 5 September 2016. Access Date: 13 January 2021. http://www.g20.utoronto.ca/2016/160905-communique.html
[2080] G20 Initiative "#eSkills4Girls," RANEPA (Moscow) 8 July 2017. Access Date: 13 January 2021. https://www.ranepa.ru/images/media/g20/2017hamburg/2017-g20-initiative-eskills4girls-en.pdf
[2081] G20 Leaders' Communique: Hangzhou Summit, G20 Information Centre (Toronto) 5 September 2016. Access Date: 13 January 2021. http://www.g20.utoronto.ca/2016/160905-communique.html
[2082] G20 Leaders' Declaration, G20 Information Centre (Toronto) 8 July 2017. Access Date: 13 January 2021. http://www.g20.utoronto.ca/2017/2017-G20-leaders-declaration.html
[2083] G20 Digital Economy Ministerial Declaration, Salta, Argentina, RANEPA (Moscow) 24 August 2018. Access Date: 13 January 2021. https://www.ranepa.ru/images/media/g20/2018buenosaires/g20_detf_ministerial_declaration_salta.pdf
[2084] G20 Leaders' Declaration, RANEPA (Moscow) 1 December 2018. Access Date: 13 January 2021. https://www.ranepa.ru/images/media/g20/2018buenosaires/buenos_aires_leaders_declaration.pdf
[2085] G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conductive to Terrorism (VECT), RANEPA (Moscow) 29 June 2019. Access Date: 13 January 2021. https://www.ranepa.ru/images/News_ciir/Project/G20_new_downloadings/G20_OSAKA_LEADERS_STATEMENT_ON_PREVENTING_EXPLOITATION_OF_THE_INTERNET_FOR_TERRORISM.pdf
[2086] Osaka Declaration on Digital Economy, RANEPA (Moscow) 29 June 2019. Access Date: 13 January 2021. https://www.ranepa.ru/images/News_ciir/Project/G20_new_downloadings/OSAKA_DECLARATION_ON_DIGITAL_ECONOMY_eng.pdf

In 2020 under Saudi Arabia's G20 presidency the ministers responsible for the digital economy adopted the G20 Roadmap toward a Common Framework for Measuring the Digital Economy. Under the Framework, the ministers proposed "an overarching policy definition of the different elements of the digital economy: The digital economy incorporates all economic activity reliant on, or significantly enhanced by the use of digital inputs, including digital technologies, digital infrastructure, digital services, and data; it refers to all producers and consumers, including government, that are utilizing these digital inputs in their economic activities."[2087]

In 2020, the DETF presented its recommendations on adjusting the United Nations 2030 Sustainable Development Goals with more than 30 indicators related to digital jobs, skills and growth in the digital economy. The recommendations were included into the OECD report "Roadmap Toward a Common Framework for Measuring the Digital Economy" that is said to "complement previous work and proposes a clear step forward for Digital Economy measurement."[2088]

Along with the Common Framework for Measuring the Digital Economy, the G20 ministers responsible for the digital economy presented three sets of best practices related to ensuring Security in the Digital Economy, advancing the G20 common Principles on the AI and promoting Smart Mobility.[2089]

In 2020 the G20 leaders' summit concluded with the joint Declaration. The leaders' recognized the key role of "connectivity, digital technologies, and policies"[2090] in "strengthening our response to the pandemic and facilitating the continuation of economic activity."[2091] As an addition to the commitment made on promotion of consumers protection, non-discriminatory environment, intellectual property rights protection and data protection, the G20 leaders noted the importance of working with stakeholders "to connect humanity by accelerating global internet penetration and bridging digital divides."[2092]

Commitment Features

The commitment focuses on issues related to digital growth: fostering open, fair, and non-discriminatory environment; protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights; and security. To achieve full compliance, the G20 member shall take steps that cover all three of the abovementioned areas.

Fostering open, fair, and non-discriminatory environment

Fostering open, fair, and non-discriminatory environment is understood as actions taken by a G20 member country aimed at promotion of a business-friendly environment that allows "foreign suppliers to compete in national markets without encountering discriminatory, excessively burdensome or restrictive conditions. It helps firms, domestic and foreign, reap the benefits of trade,

[2087] G20 Digital Economy Ministers Meeting, G20 Information Centre (Toronto) 22 July 2020. Access Date: 13 January 2021. http://www.g20.utoronto.ca/2020/2020-g20-digital-0722.html
[2088] A Roadmap Toward a Common Framework for Measuring the Digital Economy Chapter 3 'Measuring the Digital Economy: Jobs, Skills, and Growth, OECD (Paris) 2020. Access Date: 20 January 2021. http://www.oecd.org/sti/roadmap-toward-a-common-framework-for-measuring-the-digital-economy.pdf
[2089] G20 Digital Economy Ministers Meeting, G20 Information Centre (Toronto) 22 July 2020. Access Date: 13 January 2021. http://www.g20.utoronto.ca/2020/2020-g20-digital-0722.html
[2090] G20 Riyadh Summit Leaders' Declaration, G20 Information Centre (Toronto) 21 November 2020. Access Date: 13 January 2021. http://www.g20.utoronto.ca/2020/2020-g20-leaders-declaration-1121.html
[2091] G20 Riyadh Summit Leaders' Declaration, G20 Information Centre (Toronto) 21 November 2020. Access Date: 13 January 2021. http://www.g20.utoronto.ca/2020/2020-g20-leaders-declaration-1121.html
[2092] G20 Riyadh Summit Leaders' Declaration, G20 Information Centre (Toronto) 21 November 2020. Access Date: 13 January 2021. http://www.g20.utoronto.ca/2020/2020-g20-leaders-declaration-1121.html

contributing to economic growth."[2093] To promote holistic and joint approaches to openness, and mitigate negative spillovers arising from regulatory heterogeneity, the G20 actions will need to be guided by the good regulatory principles of market openness: be transparent and non-discriminatory. In the decision-making the fundamental aspect of transparency refers to the openness and inclusiveness of the policy-making process, in particular the opportunity for stakeholders to participate in formal or informal public consultations. Thus for the G20 members as policy-makers, "transparency is crucial because it enhances the efficiency of regulations by revealing the costs and benefits of policy decisions, reducing the risk of capture by specialized interests, helping remove economic distortions that might undermine domestic policy objectives, and improving public confidence in governmental and regulatory performance."[2094] Non-discrimination means that all like goods and services seeking to enter the national market, irrespective of whether digitally enabled or delivered, should have equal access, regardless of origin.[2095]

Thus, summing up, to comply with this feature of the commitment the G20 actions should be: a) transparent: helping reduce the costs of operating across different markets and clarifying the rules that apply to different products by providing up-to-date information and enabling access for different stakeholders to the policy-making process; and b) non-discriminatory: ensuring that domestic incumbents are not favored over foreign firms, or certain foreign firms over others, when operating in the digital space and selling like products in view of levelling the playing field.[2096]

Protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights

As the OECD notes in its relevant policy brief, "with the increasing complexity of the online environment, consumers may be vulnerable to actual or potential risks and challenges, which may affect their ability to participate effectively in the digital transformation."[2097] Key objectives include but not limited to "targeted policies, investment in ICT access and competencies, and education and awareness campaigns."[2098]

Examples of a state-run policies that are designed to protect and empower consumers in the digital age are as follows:

- Improvement of market monitoring and law enforcement to detect and tackle against unfair commercial practices;
- Developing targeted education and awareness programs referring to ICT literacy and ICT skills;
- Encourage consumer organizations and businesses to take into account unique issues faced by vulnerable consumers, etc.[2099]

[2093] Principles for Market Openness in the Digital Age, OECD (Paris) 21 December 2018. Access Date: 20 January 2021. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)17/FINAL&docLanguage=En
[2094] Principles for Market Openness in the Digital Age, OECD (Paris) 21 December 2018. Access Date: 20 January 2021. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)17/FINAL&docLanguage=En
[2095] Principles for Market Openness in the Digital Age, OECD (Paris) 21 December 2018. Access Date: 20 January 2021. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)17/FINAL&docLanguage=En
[2096] Principles for Market Openness in the Digital Age, OECD (Paris) 21 December 2018. Access Date: 20 January 2021. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)17/FINAL&docLanguage=En
[2097] Challenges to Consumer Policy in the Digital Age, OECD (Paris) 6 September 2019. Access Date: 19 January 2021. https://www.oecd.org/going-digital/topics/digital-consumers/challenges-to-consumer-policy-in-the-digital-age.pdf
[2098] Challenges to Consumer Policy in the Digital Age, OECD (Paris) 6 September 2019. Access Date: 19 January 2021. https://www.oecd.org/going-digital/topics/digital-consumers/challenges-to-consumer-policy-in-the-digital-age.pdf
[2099] Challenges to Consumer Policy in the Digital Age, OECD (Paris) 6 September 2019. Access Date: 19 January 2021. https://www.oecd.org/going-digital/topics/digital-consumers/challenges-to-consumer-policy-in-the-digital-age.pdf

This aspect also requires actions by the G20 members to tackle the challenges related to privacy and data protection and intellectual property rights.

Privacy and data protection

Following the OECD works on privacy and data protection such as the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,[2100], we consider that these aspects should not be treated separately.

The notion of "privacy protection" is inseparable from the notion of "laws protecting privacy" that is "national laws or regulations, the enforcement of which has the effect of protecting personal data."[2101]

Against the context of the commitment under consideration, 'data protection' refers to the notions of "consumer data" and "personal data" that are closely intertwined but do not completely overlap. The term "consumer data" is intended to capture data concerning consumers, where such data have been collected, traded or used as part of a commercial relationship.[2102] "Personal data" refers to "any information relating to an identified or identifiable individual (data subject)."[2103]

The OECD Privacy Framework suggests the following actions that could be taken by a state to promote privacy and data protection:

- Develop national privacy strategies that reflect a co-ordinated approach across governmental bodies;
- Adopt laws protecting privacy;
- Establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis;
- Encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
- Provide for reasonable means for individuals to exercise their rights;
- Provide for adequate sanctions and remedies in case of failures to comply with laws protecting privacy;
- Consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy;
- Consider the role of actors other than data controllers, in a manner appropriate to their individual role; and

[2100] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (Paris) 2013. Access Date: 19 January 2021.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[2101] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (Paris) 2013. Access Date: 19 January 2021.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[2102] Consumer Data Rights and Competition – Background note, OECD (Paris) 2013. Access Date: 19 January 2021.
https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf
[2103] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (Paris) 2013. Access Date: 19 January 2021.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

• Ensure that there is no unfair discrimination against data subjects.[2104]

The OECD also specifies the notions of "data controller" and "privacy enforcement authority" that are mentioned in the list of suggested actions.

"Data controller" means a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.[2105]

"Privacy enforcement authorities" means any public body that is responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings.[2106]

Intellectual property rights

Following the World Intellectual Property Organization's (WIPO) Handbook, we understand the "intellectual property rights" (IPR) as "the legal rights which result from intellectual activity in the industrial, scientific, literary and artistic fields."[2107] WIPO also specifies that these laws "aims at safeguarding creators and other producers of intellectual goods and services by granting them certain time-limited rights to control the use made of those productions."[2108]

Against this background, the G20 actions may refer but not limited to facilitating better legal protection of:

• Patents;

• Copyrights and related rights;

• Trademarks;

• Industrial designs and integrated circuits;

• Geographical indicators;

• IPR proprietors against unfair competition.[2109]

Security

According to the OECD "digital security" refers to "economic and social aspects of cybersecurity as opposed to purely technical aspects and those related to criminal law enforcement and national and international security."[2110] Addressing security risks is essential for economic and social prosperity. Regarding "digital security risks" the OECD notes the following:

[2104] The OECD Privacy Framework, OECD (Paris) 2013. Access Date: 19 January 2021. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[2105] The OECD Privacy Framework, OECD (Paris) 2013. Access Date: 19 January 2021. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[2106] The OECD Privacy Framework, OECD (Paris) 2013. Access Date: 19 January 2021. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[2107] WIPO Intellectual Property Handbook, WIPO (Geneva) 2004. Access Date: 13 January 2021. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_489.pdf
[2108] WIPO Intellectual Property Handbook, WIPO (Geneva) 2004. Access Date: 13 January 2021. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_489.pdf
[2109] WIPO Intellectual Property Handbook, WIPO (Geneva) 2004. Access Date: 13 January 2021. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_489.pdf
[2110] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: 19 January 2021. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf

"Digital security risk as a category of risk related to the use, development and management of the digital environment in the course of any activity. This risk can result from the combination of threats and vulnerabilities in the digital environment. They can undermine the achievement of economic and social objectives by disrupting the confidentiality, integrity and availability of the activities and/or the environment. Digital security risk is dynamic in nature. It includes aspects related to the digital and physical environments, the people involved in the activity and the organizational processes supporting it."[2111]

Ensuring the digital security requires cooperation of all "stakeholders" considered as "the governments, public and private organizations, and the individuals, who rely on the digital environment for all or part of their economic and social activities."[2112]

Accordingly to comply with this commitment feature the G20 should lead by example in implementation of a holistic public policy approach to digital security risk management and establishing co-ordination mechanisms at the domestic, regional and international levels, which ensure that all stakeholders understand digital security risk and how to manage it, take responsibility for the management of digital security, manage digital security risk in a transparent manner; co-operate, including across borders.

To foster trust and confidence in the digital environment at the national level the G20 members may implement strategies which include measures such as:

- Adopting a comprehensive framework to manage digital security risk to the government's own activities;

- Establishing co-ordination mechanisms among all relevant governmental actors to ensure that their management of digital security risk is compatible and enhances economic and social prosperity;

- Ensuring the establishment of one or more Computer Security Incident Response Team (CSIRT), also known as Computer Emergency Response Team (CERT), at national level and, where appropriate, encourage the emergence of public and private CSIRTs working collaboratively, including across borders;

- Using their market position to foster digital security risk management across the economy and society, including through public procurement policies, and the recruitment of professionals with appropriate risk management qualification;

- Encouraging the use of international standards and best practices on digital security risk management, and promoting their development and review through open, transparent and multi-stakeholder processes;

- Adopting innovative security techniques to manage digital security risk in order to assure that information is appropriately protected at rest as well as in transit, and taking into account the benefits of appropriate limitations on data collection and retention;

- Coordinating and promoting public research and development on digital security risk management with a view to fostering innovation;

[2111] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: 19 January 2021. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf
[2112] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: 19 January 2021. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf

- Supporting the development of a skilled workforce that can manage digital security risk, in particular by addressing digital security risk management in broader skills strategies. This could include fostering the development of in-service risk management training and certification and supporting the development of digital skills across the population through national education programs, notably in higher education;

- Adopting and implementing a comprehensive framework to help mitigate cybercrime, drawing on existing international instruments;

- Allocating sufficient resources to effectively implement the strategy.[2113]

Cooperation at the international level may include:

- Participating in relevant regional and international fora, and establishing bilateral and multilateral relationships to share experience and best practices; and promoting an approach to national digital security risk management that does not increase the risk to other countries;

- Providing, on a voluntary basis as appropriate, assistance and support to other countries, and establishing national points of contacts for addressing cross-border requests related to digital security risk management issues in a timely manner;

- Working to improve responses to domestic and cross-border threats, including through CSIRTs[2114] co-operation, coordinated exercises and other tools for collaboration.[2115]

The commitment requires the G20 members to support "fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security."[2116] To achieve full compliance (+1 score), a G20 member should demonstrate strong willingness to fulfil the task that implies taking actions in all three spheres that go beyond mere verbal support or participation in a discussion on a topic without further implementation in a legislative form, resources allocation, etc. Partial compliance (0 score) could be given if a G20 member takes actions either matching only one or two key areas or even all three key areas but at least one area out of three is not supported with a strong action. Also, a 0 score could be given if a G20 member takes an action matching any of three key areas, but this action could not be regarded as a strong one. We consider lack of any actions as a prerequisite for giving a G20 member a −1 score.

[2113] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: 19 January 2021. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf
[2114] Recommendations of the Council on Digital Security of Critical Activities, OECD (Paris). Access Date: 19 January 2021. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456
[2115] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: 19 January 2021. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf
[2116] Leaders' Declaration, G20 Information Centre (Toronto) 21 November 2020. Access Date: 13 January 2021. http://www.g20.utoronto.ca/2020/2020-g20-leaders-declaration-1121.html

Scoring Guidelines

−1	G20 member does no action aimed at fostering open, fair, and non-discriminatory environment; empowering and protecting consumers while addressing issues related to privacy, data protection and intellectual property rights; or addressing digital security risks.
0	G20 member takes actions in ONE or TWO of the areas: fostering open, fair, and non-discriminatory environment; empowering and protecting consumers while addressing issues related to privacy, data protection and intellectual property rights; and addressing digital security risks.
+1	G20 member takes strong actions that match all THREE areas: fostering open, fair, and non-discriminatory environment; empowering and protecting consumers while addressing issues related to privacy, data protection and intellectual property rights; and addressing digital security risks.

Compliance Director: Alexander Ignatov
Lead Analyst: Alexander Ignatov

Argentina: +1

Argentina has fully complied with the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 18 January 2021, the Public Tender 0005/2020 was opened, the bidding process for the Preventive and Corrective Maintenance of the Digital Document Management System (former GDE, Electronic Document Management), the integrated system of labeling, unique numbering, monitoring and recording of movements of all actions and files of the entire National Public Sector, which allows the complete digital processing of electronic files and is administered by the Undersecretariat of Administrative Innovation of the Ministry of Public Innovation, dependent on the Chief of Cabinet of Ministers of the Nation.[2117]

On 28 January 2021, National Director of Personal Data Protection Eduardo Cimato participated in the event for the "International Day for the Protection of Personal Data," 40th anniversary of Convention 108, carried out by the Council of Europe and the Ibero-American Data Protection Network, where the policies adopted in the context of the COVID-19 pandemic and the importance of the role of control authorities in the protection of personal data were discussed.[2118]

On 24 February 2021, the Access to Public Information Agency released a series of criteria on how the data of those people who have been vaccinated against the COVID-19 should be treated. In this sense, some of the fundamental principles of the current regulation regarding the protection of personal data and access to public information are indicated. In a context of health crisis, both in the country and worldwide, and the general shortage of vaccines, there is great public interest in knowing how they are distributed, as well as if the distribution is being carried out in accordance with the "Strategic Plan for Vaccination against COVID-19 in the Argentine Republic," published on the website of the Ministry of Health of the Nation.[2119]

[2117] Avanza la licitación de la plataforma integral de Gestión Documental Digital [The tender for the comprehensive Digital Document Management platform advances], Government of Argentina (Buenos Aires) 18 January 2021. Access Date: 13 May 2021. https://www.argentina.gob.ar/noticias/avanza-la-licitacion-de-la-plataforma-integral-de-gestion-documental-digital

[2118] Día Internacional de la Protección de Datos Personales [International Day for the Protection of Personal Data], Government of Argentina (Buenos Aires) 28 January 2021. Access Date: 13 May 2021. https://www.argentina.gob.ar/noticias/dia-internacional-de-la-proteccion-de-datos-personales

[2119] Access to information, personal data and vaccination, Government of Argentina (Buenos Aires) 24 February 2021. Access Date: 13 May 2021. https://www.argentina.gob.ar/noticias/acceso-la-informacion-datos-personales-y-vacunacion

On 23 March 2021, Secretary of Planning and Policies of Science, Technology and Innovation Diego Hurtado representing the Ministry of Science, Technology and Innovation, participated in the 2021 Korea-Latin America Digital Cooperation Forum whose central theme was the "Association for the Innovation and Digital Inclusion" organized by the Ministry of Foreign Affairs of Korea. Secretary Hurtado "celebrated the organization of this forum, the purpose of which is to consolidate efforts to share experiences in the face of digital transformation and promote Korea-Latin America cooperation in the areas of digital infrastructure, digital government, smart city and cybersecurity."[2120]

On 4 May 2021, national director of Consumer Defense Sebastián Barocelli chaired the meeting of the Technical Committee No. 7 for the Defense of the Consumer of Mercosur, on the 30th anniversary of the Treaty of Asunción. The participating authorities highlighted the central axes of the future agenda, "focused on the status of citizenship, the problem of hypervulnerable consumers, the over-indebtedness of consumers, good commercial practices among suppliers, and the need to involve civil society through academia and consumer associations. The member countries highlighted collaboration and joint work to respond to the needs of consumers."[2121]

On 2 July 2021, National Directorate for Personal Data Protection participated in the 'VIII International Data Protection Congress." organized by the Superintendency of Industry and Commerce (SIC) of Colombia and the Ibero-American Data Protection Network, with the aim of sharing opinions, experiences and recommendations of national and international experts on the protection of personal data.[2122]

On 3 August 2021, National Directorate for the Protection of Personal Data participated in a meeting of the Internal Security Council that was held by videoconference from Paraná, Entre Ríos, with the aim of analyzing the processing of geolocation data in emergency calls.[2123]

Argentina has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, Argentina receives a score of +1.

Analyst: Irina Popova

Australia: +1

Australia has fully complied with the commitment on supporting fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 9 December 2020, the Australia-Singapore Digital Economy Agreement launched. The agreement, covering such important issues as personal data protection, e-invoicing, paperless

[2120] Argentina participó del Foro de Cooperación Digital Corea-Latinoamérica 2021 [Argentina participated in the 2021 Korea-Latin America Digital Cooperation Forum], Government of Argentina (Buenos Aires) 23 March 2021. Translation provided by Google Translate. Access Date: 13 May 2021. https://www.argentina.gob.ar/noticias/argentina-participo-del-foro-de-cooperacion-digital-corea-latinoamerica-2021

[2121] Argentina encabezó el Comité Técnico de Defensa del Consumidor en los 30 años del Mercosur [Argentina headed the Technical Committee for the Defense of the Consumer in the 30 years of Mercosur], Government of Argentina (Buenos Aires) 4 May 2021. Access Date: 13 May 2021. https://www.argentina.gob.ar/noticias/argentina-encabezo-el-comite-tecnico-de-defensa-del-consumidor-en-los-30-anos-del-mercosur

[2122] Addressing the cross-border flow of personal data, Government of Argentina (Buenos Aires) 2 July 2021. Translation provided by the analyst. Access Date: 21 September 2021. https://www.argentina.gob.ar/noticias/abordaje-del-flujo-transfronterizo-de-datos-personales

[2123] Emergencies and personal data, Government of Argentina (Buenos Aires) 3 August 2021. Translation provided by the analyst. Access Date: 21 September 2021. https://www.argentina.gob.ar/noticias/emergencias-y-datos-personales

customs procedures, and electronic certification for agricultural exports, made it easier for Australian exporters to do business in Singapore.[2124]

On 6 May 2021, the Australian Government unveiled its AUD1.2 billion Digital Economy Strategy 2030, providing an outline of its policies and actions in regards to digital transformation. The strategy provided for: supporting digital skills of Australians; strengthening digital government services, including consumer protection and safety mechanisms (such as Consumer Data Act); investing in cybersecurity (over AUD50 million); supporting digital small and medium sized enterprises through tax incentives; promoting data availability and transparency.[2125]

Australia has taken actions in all three issue areas related to digital growth: fostering open, fair, and non-discriminatory environment; empowering and protecting consumers while addressing issues related to privacy, data protection and intellectual property rights; and addressing digital security risks.

Thus, Australia receives a score of +1.

Analysts: Anastasiya Kirillova and Andrei Sakharov

Brazil: +1

Brazil has fully complied with the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 2 December 2020, Federal Government published the decree of the regulatory structure of the National Data Protection Authority (ANPD), as an organ of the Presidency of the Republic, with the objective of complying with and giving effect to the General Law for the Protection of Personal Data, thus enabling adequate level of protection of the personal data of natural persons in Brazil.[2126]

On 25 February 2021, Brazilian Government affiliated technology intelligence company Serpro launched an educational platform, which offers professional training and certification for the public and private sectors in subjects related to privacy and protection of personal data.[2127]

On 22 March 2021, Ministry of Justice and Public Security, through the National Consumer Secretariat (Senacon), signed a technical cooperation agreement with the ANPD. The union of the bodies aims at the inspection and data protection of all consumers in the country.[2128]

On 30 March 2021, Law No. 14,129, which brings together the principles, rules and tools for Digital Government, was sanctioned with vetoes by President Jair Bolsonaro and published in the Official Gazette. The text establishes rules and instruments for the digital provision of public services, which

[2124] Australia-Singapore digital trade agreement kicks-off, Minister for Trade, Tourism and Investment (Barton) 9 December 2020. Access Date: 28 January 2021. https://www.trademinister.gov.au/minister/simon-birmingham/media-release/australia-singapore-digital-trade-agreement-kicks

[2125] Digital Economy Strategy 2030, Australian Government (Canberra) 6 May 2021. Access Date: 27 September 2021. https://digitaleconomy.pmc.gov.au/sites/default/files/2021-07/digital-economy-strategy.pdf

[2126] Federal Government publishes the regulatory structure of the National Data Protection Authority, Brazilian Government (Brasilia) 2 December 2020. Access Date: 12 May 2021. https://www.gov.br/anpd/pt-br/assuntos/noticias/governo-federal-publica-a-estrutura-regimental-da-autoridade-nacional-de-protecao-de-dados

[2127] Federal Government Launches Educational LGPD Platform, Serpro (Brasilia) 25 February 2021. Access Date: 12 May 2021. https://www.serpro.gov.br/menu/noticias/noticias-2021/serpro-lancamento-plataforma-lgpd

[2128]Data protection bodies come together to strengthen security, Brazilian Government (Brasilia) 20 March 2021. Access Date: 12 May 2021. https://www.gov.br/pt-br/noticias/justica-e-seguranca/2021/03/orgaos-de-protecao-de-dados-se-unem-para-reforcar-seguranca

should also be accessible in mobile applications. Access to the Digital Government platforms is free.[2129]

On 5 April 2021, the Brazilian government launched system for security control in compliance with data protection law. A tool developed by the Digital Government Secretariat of the Ministry of Economy allows the investigation of security and privacy flaws in the systems, contracts and processes in which the personal data of any citizen needed to be analyzed. Fourteen different levels of risk are ascertained automatically. It is sufficient for the citizen's data protection officer within the federal government to complete a questionnaire on the specific case online.[2130]

On 8 April 2021, the National Consumer Secretariat determined the registration of companies on the Consumidor.gov.br platform. Ordinance No. 12 was published in the Federal Official Gazette. The initiative was motivated by the significant increase in consumer demand during the coronavirus pandemic, in addition to the need for social distance in this period of exceptionality. The obligation only applies to companies or their respective economic groups if they have gross revenues of at least one hundred million reais in the last fiscal year; have reached a monthly average of 1,000 or more complaints in their customer service channels in the last fiscal year; or are sued in more than five hundred lawsuits that discuss consumer relationships. In case of non-compliance with the ordinance, false or misleading data in fulfilling the requirements, the supplier may be investigated for an infraction against the consumer protection and defense rules.[2131]

On 10 May 2021, the Ministries of Tourism and Justice launched courses on consumer rights. Tourism service providers and tourists from all over the country can enroll for free in one of the courses offered by the federal government related to consumer protection. The qualifications aim to offer legal certainty to companies and the citizen, in addition to improving the quality of consumer relations between the parties.[2132]

On 28 May 2021, the National Data Protection Authority (ANDP) published the "Guidelines for the Definitions of Personal Data Processing Agents and Supervisors." The document seeks to establish guidelines that are not binding on treatment agents and explain who can exercise the functions of controller, operator and supervisor; the legal definitions; the respective liability regimes; concrete cases that exemplify ANPD's explanations and frequently asked questions on the subject.[2133]

On 2 June 2021, Director-President of the National Data Protection Authority Waldemar Gonçalves Ortunho Júnior and the President of the Administrative Council for Economic Defense Alexandre Barreto de Souza signed Technical Cooperation Agreement destined the fight against activities that

[2129] Digital Government Law is sanctioned to increase public efficiency, Brazilian Government (Brasilia) 20 March 2021. Access Date: 12 May 2021. https://www.gov.br/economia/pt-br/assuntos/noticias/2021/marco/lei-do-governo-digital-e-sancionada-para-aumentar-eficiencia-publica

[2130] Government launches system for security control in compliance with data protection law, Brazilian Government (Brasilia) 5 April 2021. Access Date: 12 May 2021. https://www.gov.br/economia/pt-br/assuntos/noticias/2021/abril/governo-lanca-sistema-para-controle-de-seguranca-em-atendimento-a-lei-de-protecao-de-dados

[2131] National Consumer Secretariat determines the registration of companies on the Consumidor.gov.br platform, Brazilian government (Brasilia) 8 April 2021. Access Date: 12 May 2021. https://www.gov.br/mj/pt-br/assuntos/noticias/secretaria-nacional-do-consumidor-determina-o-cadastro-de-empresas-na-plataforma-consumidor-gov.br

[2132] Ministries of Tourism and Justice offer courses on consumer rights, Brazilian Government (Brasilia) 10 May 2021. Access Date: 12 May 2021. https://www.gov.br/turismo/pt-br/assuntos/noticias/ministerios-do-turismo-e-da-justica-ofertam-cursos-sobre-direitos-dos-consumidores

[2133] ANPD Publishes Guidelines On Treatment Agents And Guardians, Brazilian Government (Brasilia) 28 May 2021. Access Date: 21 September 2021. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-orientativo-sobre-agentes-de-tratamento-e-encarregado

are harmful to the economic order and the promotion and dissemination of the culture of free competition in services that claim the protection of personal data.[2134]

On 10 September 2021, ANDP and the National Consumer Secretariat of the Ministry of Justice and Public Security launched the Guide "How to protect your personal data," which focuses on consumer awareness of the importance of personal data. The material has a simplified language, in order to elucidate the themes that have great relevance, aiming to raise awareness and clarify the whole society, as it gathers information on Law No. 13,079 - the General Law for the Protection of Personal Data, with basic concepts and guidelines on consumer relations, governed by the Consumer Defense Code.[2135]

Brazil has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, Brazil receives a score of +1.

Analyst: Irina Popova

Canada: +1

Canada has fully complied with the commitment to foster an open, fair, and non-discriminatory environment, protect and empowering consumers, and address the challenges related to privacy, data protection, intellectual property rights, and security.

On 2 December 2020, Minister of Justice David Lametti introduced a Charter Statement on the Bill C-11: An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts, also known as Digital Charter Implementation Act 2020.[2136] The bill, if passed by Parliament, would introduce Consumer Privacy Protection Act, which will modernize Canada's existing private sector privacy law, and will also create the new Personal information and Data Protection Tribunal Act, which will create the Personal Information and Data Tribunal, an entity that can impose administrative monetary penalties for privacy violations. Finally, the Act will repeal Part 2 of the existing Personal Information Protection and Electronic Documents Act and turn it into stand-alone legislation, the Electronic Documents Act.[2137] A number of provisions under the proposed digital charter relate to transparency, accountability, and oversight by public institutions, attempting to limit the regulatory impact on privacy interests of citizens and businesses.[2138]

[2134] ANPD and CADE sign Technical Cooperation Agreement, Brazilian Government (Brasilia) 2 June 2021. Access Date: 21 September 2021. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-cade-assinam-acordo-de-cooperacao-tecnica

[2135] National Data Protection Authority and National Consumer Secretariat launch guide "HOW TO PROTECT YOUR PERSONAL DATA", Brazilian Government (Brasilia) 10 September 2021. Access Date: 21 September 2021. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/autoridade-nacional-de-protecao-de-dados-e-secretaria-nacional-do-consumidor-lancam-201ccomo-proteger-seus-dados-pessoais201d

[2136] Bill C-11: An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts, Government of Canada (Ottawa) 2 December 2020. Access Date: 23 November 2020. Access Date: 15 May 2021. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c11.html.

[2137] Bill summary: Digital Charter Implementation Act, 2020, Government of Canada (Ottawa) 23 November 2020. Access Date: 15 May 2021. https://www.ic.gc.ca/eic/site/062.nsf/eng/00120.html.

[2138] Bill C-11: An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts, Government of Canada (Ottawa) 2 December 2020 23 November 2020. Access Date: 15 May 2021. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c11.html

On 6 May 2021, Minister of Innovation, Science and Industry François-Philippe Champagne launched the Cyber Security Innovation Network program. Canada pledged to support the program's implementation with an investment of CAD80 million over four years, funding the creation of a national network of centers of expertise on cyber security, affiliated with post-secondary institutions, in collaboration with private sector, non-profit organizations, provincial/territorial/municipal governments and other Canadian post-secondary institutions.[2139]

On 14 May 2021, Parliamentary Secretary to the Minister of Economic Development and Official Languages and Minister responsible for Atlantic Canada Opportunities Agency Darren Fisher announced the Federal Government's CAD750,000 investment to Ignite Fredericton, a non-profit business counselling organization, to "implement a provincial cybersecurity talent development strategy."[2140]

Canada has taken actions in all three issue areas related to digital growth: fostering open, fair, and non-discriminatory environment; empowering and protecting consumers while addressing issues related to privacy, data protection and intellectual property rights; and addressing digital security risks.

Thus, Canada receives a score of +1.

Analyst: Andrei Sakharov

China: 0

China has partially complied with the commitment on supporting fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 24 November 2020, Xinhua announced the release of "Implementation Plan on Effectively Solving the Difficulties of the Elderly in Using Intelligent Technology." The plan insists on deploying new, more comprehensive and more straight-forward services for the elderly. The plan also proposes that in the future the elderly should not encounter any problems in using their smartphones. The technologies should meet all the basic needs of the elderly.[2141]

On 12 March 2021, the 14th Five-Year Plan was announced. According to the plan, China will enhance the merger of digital economy with the «real» economy. Also, the "new infrastructure" (5G, data centers, software etc.) will see enhanced investments. Moreover, artificial intelligence, big data, blockchain, cloud computing and cybersecurity were mentioned as digital industries to be fostered. The government will invest in the industries and create a good and safe environment for the development of digital economy.[2142]

On 1 May 2021, "Measures for the Supervision and Administration of Online Transactions" came into effect. The document was created in response to the issue of supervision of e-commerce. The

[2139] Government of Canada investing to position Canada as a global leader in cyber security, Government of Canada (Ottawa) 6 May 2021. Access Date: 15 May 2021. https://www.canada.ca/en/innovation-science-economic-development/news/2021/05/government-of-canada-investing-to-position-canada-as-a-global-leader-in-cyber-security.html.

[2140] Federal Government Supports Growth in Cybersecurity Sector, Government of Canada (Ottawa) 14 May 2021. Access Date: 15 May 2021. https://www.canada.ca/en/atlantic-canada-opportunities/news/2021/05/federal-government-supports-growth-in-cybersecurity-sector.html.

[2141] The General Office of the State Council issued the "Implementation Plan on Effectively Solving the Difficulties of the Elderly in Using Intelligent Technology," Xinhua (Beijing) 24 November 2020. Access Date: 28 January 2021. http://www.gov.cn/xinwen/2020-11/24/content_5563861.htm

[2142] The Fourteenth Five-Year Plan for the National Economic and Social Development of the People's Republic of China and the Outline of Long-Term Goals for 2035, Xinhua (Beijing) 12 March 2021. Access Date: 29 March 2021. http://politics.people.com.cn/n1/2021/0313/c1001-32050444.html

measures map out a series of standardized transaction behaviors and list operators' main responsibilities. The measurers will make it easier to protect the rights, interests and security of consumers.[2143]

China has addressed digital security tasks, issues related to privacy, data protection and intellectual property rights but has not taken any steps to foster open, fair, and non-discriminatory environment.

Thus, China receives a score of 0.

Analyst: Anastasiya Kirillova

France: +1

France has fully complied with the commitment on supporting fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights; and security.

In December 2020, France resumed collection of its digital tax on tech companies; starting from July 2019 the 3 per cent digital services tax applies to revenues deemed to have been generated in France by digital companies, wherever they are established, which make annual supplies of taxable services of more than EUR25 million in France and EUR750 million worldwide; in February 2020, the French tax administration confirmed that companies liable for digital tax could postpone to December 2020 the payment of the instalments due in April and October 2020; the final 2020 amount due will be paid in 2021.[2144]

On 21 January 2021, the French National Assembly adopted a draft amendment to the draft bill "Consolidating the principles of the Republic," which would have the consequence of modifying the French Law for Trust in the Digital Economy of 21 June 2004; the new obligations will apply to all platforms, whether established in France or abroad; (i) which list, rank or share content uploaded by third parties (such as social media platforms and search engines); and (ii) whose activity in France exceeds a threshold of user connections. The law is called to be in place before European-wide Digital Service Act is put in place, and will put platform operators under more onerous obligations in relation to online harmful content (including apologies of crimes or terrorism, incitement to racial or religious hatred), including cooperation with authorities in the fight against the dissemination of harmful content, implementation of reporting tools and notice action, complaint and redress mechanism, transparency reporting and risk-auditing mechanism.[2145]

On 15 February 2021, it was reported that France was pushing for the EU's upcoming regulations on Big Tech (Digital Services Act) to be changed so that member states could individually wield more power to punish bad behavior, police more types of content and force tech companies to remove illegal content (currently, only countries where tech companies have their headquarters can enforce the EU's laws).[2146]

On 31 March 2021, it was reported that according to the French highest administrative court Council of State ruling organizations can deploy legal and technical safeguards to meet their obligations under

[2143] The "Measures for the Supervision and Administration of Online Transactions" will come into effect on May 1 this year, Xinhua (Beijing) 1 May 2021. Access Date: 22 March 2021. http://www.gov.cn/xinwen/2021-03/16/content_5593218.htm
[2144] France to resume collection of digital tax, Pinsent Masons (Paris) 4 December 2020. Access Date: 30 April 2021. https://www.pinsentmasons.com/out-law/news/france-to-resume-collection-of-digital-tax
[2145] Ahead of time, online platforms may have to anticipate the Digital Service Act in France, Lexology (London) 12 February 2021. Access Date: 30 April 2021. https://www.lexology.com/library/detail.aspx?g=1174ed22-9390-40a9-8fdd-366680580810
[2146] France pushes for big changes to proposed EU tech regulation, Financial Times (London) 15 February 2021. Access Date: 30 April 2021. https://www.ft.com/content/5e41d0cf-a83c-4817-997e-a353858137ab

EU data protection law when seeking to prevent US authorities from accessing personal data stored with their outsourcing providers; the ruling was made in relation to data processing operations subject to the US surveillance framework concerning the data hosting arrangements (on Amazon's affiliate's servers in Europe) within the French vaccination program for COVID-19.[2147]

On 1 April 2021, transition period ended with respect to application of the revised French data protection supervisory authority (CNIL) guidance on the practical procedures for collecting consent concerning cookies and other trackers (issued in October 2020) – making the guidance mandatory; the Revised Guidelines provide the CNIL's guidance on how to read and comply with the relevant provisions of the Data Protection Act.[2148]

On 5 April 2021, it was reported that CNIL questioned Apple's privacy compliance, having indicated that Apple may not be obtaining proper consent when using first-party tracking methods such as cookies, which may be characterized as a potential major breach of regulations.[2149]

On 16 April 2021, it was reported that the Council of State was to decide whether to allow the widespread retention of connection data; several decrees put forward by the French government request operators to store data such as identifiers, IP addresses, names and associated addresses, and lists of telephone antennas used, for criminal investigations or national security purposes, which is assessed as breach of the EU regulation.[2150]

On 20 April 2021, it was reported that France starting from 29 April 2021 would become the first EU country to start testing digital COVID-18 travel certificates as part of a Europe-wide scheme that Brussels hopes will allow people to travel more freely within the bloc by the summer.[2151]

In February 2021, it was reported that President Emmanuel Macron pledged to allocate new investment (in different sources from EUR500 million to EUR1 billion for development of France's national security strategy and assisting companies and public authorities boost their cyber defense capabilities; it was further reported that President Macron set the goal to triple the annual sales of French cyber-security companies to EUR25 billion in 2025 from EUR7.3 billion in 2019, and double the number of jobs in the sector by 2025.[2152, 2153] In the same month, France launched the ExpertCyber initiative that certifies French companies that both install and maintain security products, as well as provide incident response services; organizations in any sector can use the ExpertCyber directory to check whether a particular company is certified, or to search for providers that meet their specific requirements; dozens of service providers have apparently been convinced

[2147] French GDPR ruling addresses US surveillance powers, Pinsent Masons (Paris) 31 March 2021. Access Date: 30 April 2021. https://www.pinsentmasons.com/out-law/news/french-gdpr-ruling-addresses-us-surveillance-powers

[2148] France: The cookies transition period will end in a few days – starting April 1st, organizations must comply with the CNIL's revised guidelines on cookies and trackers, Lexology (London) 23 March 2021. Access Date: 30 April 2021. https://www.lexology.com/library/detail.aspx?g=f10f5a9a-46aa-407b-9616-6a09a057d14a

[2149] France's Data Protection Authority Has Questions About Apple's Privacy Compliance, CPO Magazine (Singapore) 5 April 2021. Access Date: 30 April 2021. https://www.cpomagazine.com/data-protection/frances-data-protection-authority-has-questions-about-apples-privacy-compliance/

[2150] France to decide whether to allow widespread retention of connection data, Euractiv (Brussels) 16 April 2021. Access Date: 30 April 2021. https://www.euractiv.com/section/data-protection/news/france-to-decide-whether-to-allow-widespread-retention-of-connection-data/

[2151] France is first EU member state to start testing digital Covid travel certificate, The Guardian (London) 20 April 2021. Access Date: 30 April 2021. https://www.theguardian.com/world/2021/apr/20/france-is-first-eu-member-state-to-start-testing-digital-covid-travel-certificate

[2152] France to Boost Cyber Security Defenses After Attacks, Insurance Journal (San Diego) 18 February 2021. Access Date: 30 April 2021. https://www.insurancejournal.com/news/international/2021/02/18/601658.htm

[2153] Emmanuel Macron pledges €1bn for cybersecurity after hospital ransomware attacks, Healthcare IT News (Portland) 22 February 2021. Access Date: 30 April 2021. https://www.healthcareitnews.com/news/emea/emmanuel-macron-pledges-1bn-cybersecurity-after-hospital-ransomware-attacks

that the ExpertCyber label might give them an edge when pitching for business from organizations contending with surging ransomware attacks and an attack surface enlarged for COVID-19-related reasons.[2154]

On 6 May 2021, it was reported that French Expertise Centre for Digital Regulation and the Directorate General for Enterprise signed a scientific partnership agreement for digital regulation. The move provides an opportunity to take stock of the needs of government departments in this area, and to focus on the development of methods and algorithms to support them in their monitoring of the practices of these digital platforms.[2155]

On 7 June 2021, the French Autorité de la Concurrence delivered the first-ever decision in the world establishing that Google's ad tech practices are in breach of EU competition law. The decision resulted from an investigation launched after Geradin Partners filed a complaint before the Autorité on behalf of News Corp (owner of among others The Wall Street Journal and The Times) in summer 2019. The decision was adopted within the context of a so-called "transaction procedure" available in France, according to which Google agreed not to contest the charges of the Autorité. The decision imposed on Google a fine of EUR220 million and rendered binding a series of commitments proposed by Google.[2156]

On 18 June 2021, Secretary of State for the Digital Economy Cédric O announced more regulation was needed to control a tech industry that is "evolving as an oligopoly." Speaking at the VivaTech 2021 conference in Paris, he said national governments were beginning to realize that big tech companies were not putting the public interest first and that more regulation is needed "both on competition and on the economic side, but also on the content regulation side."[2157]

On 22 July 2021, CNIL published its decision, of 20 July 2021, whereby it imposed a fine of EUR1.75 million on AG2R La Mondiale, a mutual insurance group company, for violations of right to be informed and storage limitation principle, following an audit carried out in 2019. In particular, the decision outlines that AG2R La Mondiale had stored the data belonging to millions of prospective and current clients for an excessive period as it had not complied with the required time periods.[2158]

On 29 July 2021, it was reported that the CNIL fined the SOCIÉTÉ DU FIGARO EUR50,000 for depositing advertising cookies on the lefigaro.fr website without obtaining the prior consent of Internet users. The CNIL, after receiving a complaint, carried out several checks between 2020 and 2021 on the news website lefigaro.fr. These checks revealed that when a user visited this site, cookies were automatically placed on his computer by the company's partners, without any action on his part

[2154] French certification scheme for infosec service providers off to promising start, The Daily Swig (Manchester) 31 March 2021. Access Date: 30 April 2021. https://portswigger.net/daily-swig/french-certification-scheme-for-infosec-service-providers-off-to-promising-start

[2155] The regulation of digital platforms: French government takes the lead, Inria (Rocquencourt) 6 May 2021. Access Date: 24 September 2021 https://www.inria.fr/en/regulation-digital-platforms-pere-regalia

[2156] Google fined € 220 million by French competition authority over abusive ad tech practices, Geradin partners acting for complainant news corp, Geradin Partners (Brussels) 14 June 2021. Access Date: 24 September. https://www.geradinpartners.com/google-fined-e-220-million-by-french-competition-authority-over-abusive-ad-tech-practices-geradin-partners-acting-for-complainant-news-corp/

[2157] VivaTech 2021: Cédric O says tech 'oligopoly' must be regulated to defend the public interest, Euronews (Lyon) 18 June 2021. Access Date: 24 September 2021. https://www.euronews.com/next/2021/06/18/vivatech-2021-cedric-o-says-tech-oligopoly-must-be-regulated-to-defend-the-public-interest

[2158] France: CNIL imposes €1.75M fine to AG2R La Mondiale for violations of right to be informed and storage limitation principle, DataGuidlines (Atlanta) 23 July 2021. Access Date: 24 September 2021. https://www.dataguidance.com/news/france-cnil-imposes-%E2%82%AC175m-fine-ag2r-la-mondiale

or despite his refusal. Several of these cookies were used for advertising purposes and should have been subject to the user's consent.[2159]

France has taken actions in all three issue areas related to digital growth: fostering open, fair, and non-discriminatory environment; empowering and protecting consumers while addressing issues related to privacy, data protection and intellectual property rights; and addressing digital security risks.

Thus, France is awarded a score of +1.

Analyst: Pavel Doronin

Germany: +1

Germany has fully complied with the commitment on supporting fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 16 December 2020, Germany passed a draft bill for a "Second Bill To Increase The Security of Information Technology Systems." The purpose was to implement proceedings to avert threats to cyber and information security for the state, the economy and society including Significant extension of the powers of the Federal Office for Information Security and Expansion of obligations affecting operators of critical infrastructures and companies of special public interest.[2160]

On 19 January 2021, the 10th Amendment of the German Competition Act entered into force. It was implemented to provide the German Federal Cartel Office with an efficient instrument against alleged digital monopolists to keep digital markets open. The Amendment also introduced changes to the German Competition Act concerning antitrust investigations procedure cartel damage claims.[2161]

On 19 January 2021, the German government announced initiative on the rolling out gigabit capable internet connections nationwide by 2025 and to ensure across-the-board mobile communications coverage.[2162]

On 19 January 2021, Germany unveiled another coronavirus stimulus package, with EUR50 billion for a raft of projects addressing climate change, innovation, solar and wind power, and digitization.[2163]

Germany has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, Germany receives a score of +1.

Analyst: Sergei Vasilkovsky

[2159] Cookies: 50.000 euro GDPR-fine against SOCIÉTÉ DU FIGARO by the French CNIL, CNIL (Paris) 29 July 2021. Access Date: 24 September 2021. https://www.cnil.fr/en/cookies-penalty-50000-euros-against-societe-du-figaro
[2160] Regulatory Pressure For Cybersecurity Increases: Key Aspects of the German Federal Government's Draft Bill for an IT Security Act 2.0 and Next Steps in the Legislative Process (Berlin) 16 December 2020. Access Date: 14 May 2021. https://www.lexology.com/library/detail.aspx?g=b3fc4c47-2835-44d0-9775-fb8ffe2dee0a
[2161] "Digitalization Act": Significant Changes to German Antitrust Rules, Gibson Dunn (Berlin) 28 January 2021. Access Date: 14 May 2021. https://www.gibsondunn.com/digitalization-act-significant-changes-to-german-antitrust-rules/
[2162] Resolving the crisis, progressing with structural transformation, the Federal Government (Berlin) 28 January 2021. Access Date: 14 May 2021. https://www.bundesregierung.de/breg-en/news/annual-economic-report-2021-1845890
[2163] Resolving the crisis, progressing with structural transformation, the Federal Government (Berlin) 28 January 2021. Access Date: 14 May 2021. https://www.bundesregierung.de/breg-en/news/annual-economic-report-2021-1845890

India: 0

India has partially complied with the commitment on supporting fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 24th November 2020, India released the list of 43 mobile apps, deemed a threat to public and national security, that will be blocked in India, including e-commerce apps.[2164]

On 9th December 2020, India, together with Better Than Cash Alliance, co-organized a joined Peer Exchange in order to promote digital payments and to work jointly towards the goal of "Digital India for all."[2165]

On 21 June 2021, India proposed Amendments to the Consumer Protection (E-commerce) Rules adopted in 2020. Proposed amendments aim to bring transparency in e-commerce platforms and further strengthen the regulatory regime.[2166]

India has addressed digital security tasks, issues related to fostering open, fair, and non-discriminatory environment, but has not taken any steps to fight the issue of privacy, data protection and intellectual property rights.

Thus, India receives a score of 0.

Analysts: Anastasiya Kirillova and Irina Popova

Indonesia: +1

Indonesia has fully complied with the commitment on supporting fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 29 December 2020, the Central Bank issued Regulation No. 22/23/PBI/2020 pertaining to the restructuring of the regulatory framework of payment systems, including the reclassification of the activities of payment service operators, and shifting the regulatory framework from an entity-based approach to activity and risk-based approach, enabling Central Bank to better mitigate potential risks in the country's financial system; the regulation also issues new requirements with regards to share ownership and capital, which could impact foreign investors in the payment services industry. The regulation is part of the Indonesia 2025 Payment System Blueprint aimed at supporting banking digitalization, integration of the digital economy and interlink between fintech and the banking sector, as well as ensuring innovation, consumer protection, and healthy business competition, and safeguarding national interests in cross-border digital economy and finance transactions.[2167]

On 16 February 2021, it was reported that the Financial Services Authority (OJK) was to release the guidelines for digital banks operations by the middle of 2021; instead of detailed regulation OJK

[2164] Government of India blocks 43 mobile apps from accessing by users in India, Public Information Bureau (Delhi) 24 November 2020. Access Date: 1 February 2021. https://pib.gov.in/PressReleasePage.aspx?PRID=1675335
[2165] India and UN-Based Better Than Cash Alliance organized a joint Peer learning exchange on fintech solutions for responsible digital payments at the last mile, Public Information Bureau (Delhi) 9 December 2021. Access Date: 1 February 2021. https://pib.gov.in/PressReleasePage.aspx?PRID=1679436
[2166] Proposed Amendments to the Consumer Protection (E-commerce) Rules, 2020, Public Information Bureau (Delhi) 21 June 2021. Access Date: 21 September 2021. https://pib.gov.in/PressReleasePage.aspx?PRID=1729201
[2167] Bank Indonesia Issues Regulation on Payment Systems, ASEAN Briefing (Jakarta) 18 January 2021. Access Date: 30 April 2021. https://www.aseanbriefing.com/news/bank-indonesia-issues-regulation-on-payment-systems/

made a choice for the set of guiding principles on how banks operate digitally and mitigate any of their risks that may occur.[2168]

On 13 April 2021, President Joko Widodo issued a presidential executive order to augment the institutional authority of the National Cyber and Crypto Agency as an agency reporting directly to the president, enhancing both its agility and authority outside individual ministry, and coordinating ministry frameworks, and to strengthen the agency's structure, functions, responsibilities and funding base, thereby boosting its efficiency and enhancing national security, sovereignty, and data protection. The above decree is expected to be followed by three related decrees pertaining to the release of Indonesia's first national cybersecurity strategy 2020-24, the management of national cyber crises, and vital national information infrastructure.[2169]

On 3 May 2021, it was reported that the Commodity Futures Trade Regulatory Agency proposed imposing a final income tax on any transaction involving a digital currency on licensed exchanges; the proposal was at the time under review by other regulators.[2170]

On 12 July 2021, the Directorate General of Taxes (DGT) has revealed that USD114 million (IDR1.65 trillion) was recouped in the first half of 2021 as a result of the VAT rules that apply to the cross-border supply of digital services. The figures released by the DGT show a 125 per cent increase since the second half of 2020 as well as a significant increase in the number of additional digital businesses that had been nominated as VAT collectors by the DGT. [2171]

On 30 July 2021, it was reported that the Indonesian Business Competition Supervisory Commission (KPPU) issued a regulation at the end of May 2021 on the enforcement of fines for monopolistic practices and unfair business competition. KPPU Regulation No. 2 of 2021 aims to provide certainty in the enforcement of administrative fines regulated under Government Regulation No. 44 of 2021 regarding the Implementation of the Prohibition of Monopolistic Practices and Unfair Business Competition to conform with the provisions in the Omnibus Law.[2172]

On 11 August 2021, it was reported that the Asian and Pacific Training Centre for Information Communications Technology for Development conducted a virtual seminar on Data Protection and Privacy for Indonesia. The event was co-organized with the Ministry of Communications and Informatics of the Republic of Indonesia. The webinar's aim was to enhance understanding among policymakers, regulators and civil servants on the importance of data privacy and protection; emphasize the role of data privacy legislation; and share information on international frameworks. Sessions also discussed the data privacy laws and regimes of the Republic of Korea, Singapore and other selected countries, and contributed to Indonesia's efforts for strengthening data protection and privacy in the country.[2173]

[2168] Guidelines for digital banks in Indonesia to be released by mid-year, The Straits Times (Singapore) 16 February 2021. Access Date: 30 April 2021. https://www.straitstimes.com/asia/se-asia/guidelines-for-digital-banks-in-indonesia-to-be-released-by-mid-year

[2169] Indonesia responds to the cyber dark side, Lowy Institute (Sydney) 13 May 2021. Access Date: 15 May 2021. https://www.lowyinstitute.org/the-interpreter/indonesia-responds-cyber-dark-side

[2170] Indonesia proposes tax on digital currency transactions, Coingeek (Montreal) 3 May 2021. Access Date: 15 May 2021. https://coingeek.com/indonesia-proposes-tax-on-digital-currency-transactions/

[2171] Indonesia tax on digital services raises USD114m in first half of 2021, TAXAMO (Kerry) 12 July 2021. Access Date: 24 September 2021. https://blog.taxamo.com/insights/indonesia-tax-digital-services

[2172] Indonesia: Indonesia's Business Competition Body Issues New Regulation On Enforcement Of Fines, Mondaq (New York) 30 July 2021. Access Date: 24 September 2021. https://www.mondaq.com/antitrust-eu-competition-/1097666/indonesia39s-business-competition-body-issues-new-regulation-on-enforcement-of-fines

[2173] Indonesia Webinar on Data Protection and Privacy, APCICT (Inchon) 11 August 2021. Access Date: 24 September 2021. https://www.unapcict.org/news/indonesia-webinar-data-protection-and-privacy

On 17 August 2021, it was published that Indonesia's digital economy expanded by 11 per cent to USD44 billion in 2020 from USD40 billion in 2019, showing resilience amid the Covid-19 pandemic, according to Mrs Hastin Dumadi, Head of the Economic Department in the Embassy of Indonesia in Singapore. The digital economy contributed 4 per cent of the country's gross domestic product in 2020. By 2030, Indonesia's digital economy is projected to be accelerating at over 23 per cent compound annual growth rate.[2174]

On 24 August 2021, the Indonesian government set a target that the country's digital economic growth may account for around 40 per cent of the digital economy market in ASEAN by 2025. Trade Minister Muhammad Lutfi made the remark during a meeting with the Commission VI of the House of Representatives of Indonesia.[2175]

Indonesia has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, Indonesia receives a score of +1.

Analyst: Pavel Doronin

Italy: +1

Italy has fully complied with the commitment to foster an open, fair, and non-discriminatory environment, protect and empowering consumers, and address the challenges related to privacy, data protection, intellectual property rights, and security.

On 25 April 2021, the Government of Italy presented the National Recovery and Resilience Plan to the Parliament. The plan is a part of the European Next Generation EU EUR750 billion package, aimed at environmental transition and carbon-neutral recovery from the pandemic-induced crisis. EUR40.32 billion of the EUR191.5 billion Italian package (around 27 per cent) are to be spent on the digitalization priorities. Among them are: migration to the cloud of central and local public administrations; creating a national infrastructure and supporting administrations in the transformation path; enhanced interoperability between government data; digitization of key procedures/user interfaces; state-of-the-art digital services for citizens; strengthening cybersecurity; enhancing citizens' basic digital skills; introducing new regulatory framework to speed up procurement of information and communications technologies and encourage interoperability by administrations; supporting justice reform interventions through investments in digitization and management of the backlog of cases.

On 30 April 2021, the Ministry of Technological Innovation and Digital Transition put forward the "Italia Digitale 2026" program to support the implementation of the National Recovery and Resilience Plan.[2176] The five goals under the program are: spread digital identity, ensuring it is used by 70 per cent of the population; close the digital skills gap, with at least 70 per cent of the population being digitally skilled; bring about 75 per cent of Italian public administration offices to use cloud services; achieve at least 80 per cent of essential public services delivered online; ensure universal

[2174] Indonesia's digital economy grows to US$44 billion, The Business Times (Singapore) 17 August 2021. Access Date: 24 September 2021. https://www.businesstimes.com.sg/hub/indonesia-76th-independence-day/indonesias-digital-economy-grows-to-us44-billion

[2175] Indonesian aims for 40 per cent of Asean's digital economy market share by 2025, The Star (Jakarta) 24 August 2021. Access Date: 24 September 2021. https://www.thestar.com.my/aseanplus/aseanplus-news/2021/08/24/indonesian-aims-for-40-per-cent-of-asean039s-digital-economy-market-share-by-2025

[2176] Next Generation Italia, the government plan approved, Italian Ministry of Technological Innovation and Digital Transition (Rome) 30 April 2021. Access Date: 17 May 2021. https://innovazione.gov.it/notizie/articoli/next-generation-italia-approvato-il-piano-del-governo/

access to ultra-wideband networks.[2177] "Italia Digitale 2026" also provided for the implementation of the National Cyber Security Perimeter framework over the upcoming five years. Its objectives include increasing cyber protection of public administration offices and critical infrastructure; strengthening technical capabilities for the continuous assessment and audit of the security of electronic equipment and applications used for the provision of critical services; and enhancing skills of law enforcement and public security personnel.[2178]

Italy has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, Italy receives a score of +1.

Analyst: Andrei Sakharov

Japan: +1

Japan has fully complied with the commitment on supporting fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 24 November 2020, an appeal for opinions was announced on a draft revision to the Guidelines for Promotion of Competition in the Telecommunications Business Field.[2179]

On 18 December 2020, another appeal for opinions was announced on draft revision to the Guidelines for Promotion of Competition in the Telecommunications Business Field. On the same date, guidelines based on previously shared opinions were released with an ordinance to four telecommunications carrier-related associations to start complying with them.[2180]

On 2 December 2020, the Ministry of Internal Affairs and Communications announced establishment of the Internet Traffic Study Group to discuss and study various issues on the Internet route from an overall perspective to ensure the quality of internet services and appealed for public proposals on various issues on the Internet route and countermeasures.[2181]

On 4 December 2020, the Ministry of Internal Affairs and Communications announced appeal for opinions on draft revision to Commentary for Guidelines for Protection of Personal Information in Telecommunications Business, a draft of the Guidelines for Issuance of a Business Improvement

[2177] Digital Italy 2026, Italian Ministry of Technological Innovation and Digital Transition (Rome) 30 April 2021. Access Date: 17 May 2021. https://innovazione.gov.it/dipartimento/focus/italia-digitale-2026/#gli-obiettivi-italia-digitale-2026
[2178] The strategic role of Cybersecurity, Ministry of Technological Innovation and Digital Transition (Rome) 30 April 2021. Access Date: 17 May 2021. https://innovazione.gov.it/notizie/articoli/il-ruolo-strategico-della-cybersecurity/
[2179] Appeal for Opinions on Draft Revision to Guidelines for Promotion of Competition in the Telecommunications Business Field, Ministry of Internal Affairs and Communications (Tokyo) 24 November 2020. Access Date: 30 April 2021. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2020/11/24_04.html
[2180] Appeal for Opinions on Draft Revision to Guidelines for Promotion of Competition in the Telecommunications Business Field, Release of Revised Guidelines, and Request for Compliance with Guidelines, Ministry of Internal Affairs and Communications (Tokyo) 18 December 2020. Access Date: 30 April 2021. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2020/12/18_09.html
[2181] Appeal for Proposals to Ensure the Quality of Internet Services in New Daily Lives, Ministry of Internal Affairs and Communications (Tokyo) 2 December 2020. Access Date: 30 April 2021. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2020/12/02_02.html

Order to Prevent Hindrance in Ensuring the Secrecy of Communications, and a draft Reference Document on How to Obtain Consent.[2182]

On 25 December 2020, the Ministry of Internal Affairs and Communications released Master Plan 3.0 on the Regional Development of Information Communications and Technology (ICT) Infrastructure, providing for infrastructure development in disadvantaged areas for ICT and accelerated development of 5G infrastructure.[2183]

On 3 June 2020, the Act to Improve the Transparency and Fairness of Specified Digital Platforms was promulgated. The act brings significant effect on the business practices of certain digital platform operators active in the Japanese market as it requires them to: (i) disclose information such as terms and conditions of their transaction with counter parties (such as merchants operating online stores on the digital platforms); (ii) develop fair procedures and systems; and (iii) submit an annual report on their business operations to the Ministry of Economy, Trade and Industry.[2184] It also empowers the government to assess compliance, publicize the results of its assessment, and take necessary actions to enforce compliance, including issuing fines for violations. The act provides that it will become effective on or before 2 June 2021.[2185] The act's enforcement date was later stipulated by Japan's Cabinet as 1 February 2021.[2186]

On 15 January 2021, Japan signed its first of such kind Comprehensive Memorandum of Cooperation in the Field of Information and Communications Technology with the Ministry of Communications of the Republic of India, which contains among others provisions on cyber security.[2187]

On 22 January 2021, the State Minister for Internal Affairs and Communications presented the ASEAN-Japan ICT Work Plan 2021 on cooperation and collaboration in the ICT field between Japan and the Association of Southeast Asian Nations (ASEANS), which contains among others provisions on cyber security.[2188]

On 26 January 2021, the Cabinet in its order defined categories and scales of businesses to designate "specified digital platforms" under the Act to Improve the Transparency and Fairness of Specified Digital Platforms; in particular, (i) businesses operating comprehensive online shopping malls selling goods and having sales of 300 billion yen or more per fiscal year in Japan, and (ii) businesses

[2182] Appeal for Opinions on Draft Revision to Commentary for Guidelines for Protection of Personal Information in Telecommunications Business, Ministry of Internal Affairs and Communications (Tokyo) 4 December 2020. Access Date: 30 April 2021. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2020/12/04_03.html
[2183] Release of Master Plan 3.0 on the Regional Development of ICT Infrastructure, Ministry of Internal Affairs and Communications (Tokyo) 25 December 2020. Access Date: 30 April 2021.
https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2020/12/25_01.html
[2184] Global competition around the world: Japan, Lexology (London) 3 December 2020. Access Date: 30 April 2021.
https://www.lexology.com/library/detail.aspx?g=76fd2569-c913-466c-af3c-83d5f570cd71
[2185] Japanese Legislature Passes Act to Regulate Big Tech Platforms, Winston and Strawn LLP (Chicago) 18 December 2020. Access Date: 30 April 2021. https://www.winston.com/en/competition-corner/japanese-legislature-passes-act-to-regulate-big-tech-platforms.html#!/closed_state
[2186] Cabinet Decisions Made on Two Cabinet Orders for the Act on Improving Transparency and Fairness of Digital Platforms, Ministry of Economy, Trade and Industry (Tokyo) 26 January 2021. Access Date: 30 April 2021.
https://www.meti.go.jp/english/press/2021/0126_003.html
[2187] Signing of the First Comprehensive Memorandum of Cooperation in the Field of Information and Communications Technology with the Ministry of Communications of the Republic of India, Japan's Ministry of Internal Affairs and Communications 15 January 2021. Access Date: 30 April 2021.
https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2021/1/15_07.html
[2188] Result of First ASEAN Digital Ministers' Meeting with Japan, Japan's Ministry of Internal Affairs and Communications 22 January 2021. Access Date: 30 April 2021.
https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2021/1/25_01.html

operating application stores and having sales of 200 billion yen or more per fiscal year in Japan were defined as those subject to the act.[2189]

On 1 February 2021, new measures by Japanese government became effective to improve the transparency and fairness of digital platforms. It sets out principles for certain digital platform providers identified according to the size of their sales in Japan (JPY300 billion for B-to-C shopping malls and JPY200 billion for B-to-C application stores).[2190]

On 4 February 2021, the Ministry of Economy, Trade and Industry (METI) established a study group on the "digital industry" to discuss ways to accelerate digital transformation in business, and achieve growth by providing new value to society while coping with changes in the global competitive environment.[2191] Further, on 1 March 2021, METI established a study group on international taxation in the digital economy to elaborate ideal approaches to fair international taxation that contributes to enhancement of Japanese companies' competitiveness and vitalization of the Japanese economy amid the acceleration of economic digitalization.[2192]

On 24 February 2021, the 26th EU-Japan ICT dialogue meeting took place: Japan presented its efforts to improve 5G security, and the Smart City Information Security Guidelines, while the EU expressed interest in Japan's call for cooperation through the activities of the ASEAN-Japan Cybersecurity Capacity Building Centre; the parties agreed to continue exchanging opinions in the field of cybersecurity.[2193]

On 26 February 2021, the Ministry of Internal Affairs and Communications 2021 recipients of Cybersecurity Encouragement Prizes of Minister for Internal Affairs and Communications; the Ministry has been recognizing individuals and organizations showing outstanding achievements in the forefront fields of cybersecurity since 2017.[2194]

On 4 March 2021, the National Police Agency, the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry jointly released the Report on the Status of the Occurrence of Acts of Unauthorized Computer Access and the Progress of Research and Development on Technology Relating to Access Control Features, as part of their efforts to develop environments that hinder unauthorized computer access in order to prevent crimes.[2195]

From 8 to 12 March 2021, METI and the Industrial Cyber Security Center of Excellence under the Information-technology Promotion Agency, in collaboration with the government of the United States hosted the Japan-US Industrial Control Systems Cybersecurity Week; as an integral part of the

[2189] Cabinet Decisions Made on Two Cabinet Orders for the Act on Improving Transparency and Fairness of Digital Platforms, Ministry of Economy, Trade and Industry (Tokyo) 26 January 2021. Access Date: 30 April 2021. https://www.meti.go.jp/english/press/2021/0126_003.html

[2190] WTO Report on G20 Trade Measures (mid-October 2020 to mid-May 2021), WTO OMC (Washington DC) 28 June 2021. Access Date: 24 September 2021. https://www.wto.org/english/news_e/news21_e/report_trdev_jun21_e.pdf

[2191] Study Group on Creation of Digital Industry to be Inaugurated, Ministry of Economy, Trade and Industry (Tokyo) 4 February 2021. Access Date: 25 April 2021. https://www.meti.go.jp/english/press/2021/0204_001.html

[2192] "Study Group on International Taxation in the Digital Economy" to be Inaugurated, Ministry of Economy, Trade and Industry (Tokyo) 1 March 2021. Access Date: 30 April 2021. https://www.meti.go.jp/english/press/2021/0301_001.html

[2193] Result of 26th Japan-EU ICT Policy Dialogue, Ministry of Internal Affairs and Communications (Tokyo) 26 February 2021. Access Date: 30 April. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2021/2/26_07.html

[2194] Announcement of Recipients of Cybersecurity Encouragement Prizes of Minister for Internal Affairs and Communications, Ministry of Internal Affairs and Communications (Tokyo) 26 February 2021. Access Date: 30 April 2021. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2021/2/26_08.html

[2195] Report Compiled on the Status of the Occurrence of Acts of Unauthorized Computer Access and the Progress of Research and Development on Technology Relating to Access Control Features, Ministry of Economy, Trade and Industry (Tokyo) 4 March 2021. Access Date: 30 April 2021. https://www.meti.go.jp/english/press/2021/0304_004.html

Cybersecurity Week, Japan, the US, and the European Union have for the first time launched the Japan-US-EU seminars on cybersecurity in the post-COVID environment.[2196]

On 1 April 2021, METI formulated the Cyber/Physical Security Guidelines for the Safety and Security of Smart Homes. The guidelines organize matters regarding cyber/physical security measures in smart homes and the minimum necessary measures that each stakeholder should consider. In order to meet the needs of stakeholders with diverse knowledge and backgrounds, the guidelines group the security measures into stages, from simple countermeasure guides to specific countermeasure requirements and comparisons with international standards.[2197]

On 30 April 2021, METI presented the results of its examination of measures to ensure the sustainability of Japanese filmmaking, including improving the business and working environment for freelancers. Detailed studies of the issues involved in enhancing fairness at film production worksites were conducted from August 2020 to March 2021 through various bodies created for the purpose. Specifically, a preparatory committee was set up for establishing an Organization for Enhancing Fair Film Production (provisional name), and this was accompanied by working groups formed to study the following specialized areas: system design; formulating certification standards; and measures for human resource development, etc.[2198]

On 21 June 2021, it was reported that recognizing the need for standards aimed at ensuring the safety and security of an IoT society being recognized internationally, Japan had proposed a standard based on the IoT Security Guidelines, etc. and a standard based on the IoT Security Guidelines, General Framework for Secure IoT Systems, and the IPA's "IoT" series. The former was proposed to ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection), and the latter to ISO/IEC JTC1/SC41 (Internet of things and digital twin).[2199]

On 3 August 2021, Japan's Personal Information Protection Commission published its long-awaited Guidelines to amendments enacted in 2020 (the "2020 amendments") to Japan's Act on the Protection of Personal Information (APPI). While many of the 2020 amendments do not take effect until 1 April 2022, they aim of APPI, among other things, is to strengthen penalties (these amendments took effect in 2020), introduce mandatory reporting of certain breaches, strengthen the extraterritorial application of the APPI, and expand the scope of data that is protected under the APPI.[2200]

On 6 August 2021, it was reported that Japan issued the outline for its "Next Cyber Strategy" on the 7 July 2021, to be approved by Cabinet within 2021. This strategy has a three-year planning period and has been prepared in the backdrop of increasing cyber-attacks from China stemming from deteriorating relations over Taiwan. This strategy has been formalized after soliciting public comments by the special task force on cybersecurity strategies headed by Chief Cabinet Secretary

[2196] Japan-US Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region in FY2020, Ministry of Economy, Trade and Industry (Tokyo) 15 March 2021. Access Date: 30 April 2021. https://www.meti.go.jp/english/press/2021/0315_001.html
[2197] Cyber/Physical Security Guidelines for the Safety and Security of Smart Homes Formulated, Japan's Ministry of Economy, Trade and Industry (Tokyo) 1 April 2021. Access Date: 24 September 2021. https://www.meti.go.jp/english/press/2021/0401_004.html
[2198] Report Compiled on Enhancing Fairness at Film Production Worksites, Japan's Ministry of Economy, Trade and Industry (Tokyo) 30 April 2021. Access Date: 24 September 2021. https://www.meti.go.jp/english/press/2021/0430_002.html
[2199] New International Standard for Safe Use of IoT Products and Systems Issued, Japan's Ministry of Economy, Trade and Industry (Tokyo) 21 June 2021. Access Date: 24 September 2021. https://www.meti.go.jp/english/press/2021/0621_003.html
[2200] Official Guidelines issued for Japan's upcoming data privacy law amendments, JDSupra (San Francisco) 31 August 2021. Access Date: 24 September 2021. https://www.jdsupra.com/legalnews/official-guidelines-issued-for-japan-s-8097428/

Katsunobu Kato, with the goal to "enhance defense, deterrence and assessment capabilities and strengthen cooperation among relevant bodies to protect security interests".[2201]

On 19 August 2021, it was reported that a total of six meetings of the "Study Group on International Taxation in the Digital Economy" had been held since March this year. The outcomes have now been compiled into an interim report, which is to be published later in 2021. [2202]

Japan has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, Japan receives a score of +1.

Analyst: Pavel Doronin

Korea: +1

Korea has fully complied with the commitment on supporting fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 7 December 2020, the Financial Services Commission unveiled its plans to introduce a routine inspection of personal data protection at financial institutions to ensure consistency in data protection and improve accountability. The plans include establishing specific inspection standards according to the data lifecycle, providing feedbacks on a regular basis through Financial Security Institute and setting up self-inspection guidelines for financial institutions.[2203]

On 6 January 2021, the Government of Korea presented the 2021 Action Plan for Digital New Deal. The Digital New Deal is a national innovation project that invests a total of KRW58.2 trillion (approximately USD51.6 billion) into advance data, network and AI-based economic structure, digital infrastructure and regulatory reform. The government aims to create 900,000 new jobs in information communications and technology (ICT)-related spheres by 2025.[2204]

On 25 February 2021, the Government of Korea presented the 4th Basic Plan for Nurturing and Supporting Scientific Talents for 2021 – 2025 period. The Plan outlines three main policy goals: attract talents with capabilities to respond to future changes; sustain and expand the scientific talent pool; and advance ecosystem for "transforming into a country that attracts talented workforce." The Ministry of Science and ICT estimated a total of more than KRW25 trillion (approximately USD22.2 billion) would be invested from relevant departments and local governments to support 180

[2201] Japan's new cyber security strategy: Significant dimensions, The Times of India (Mumbai) 6 August 2021. Access Date: 24 September 2021. https://timesofindia.indiatimes.com/blogs/ChanakyaCode/japans-new-cyber-security-strategy-significant-dimensions/

[2202] Interim Report of "Study Group on International Taxation in the Digital Economy" Compiled, Japan's Ministry of Economy, Trade and Industry (Tokyo) 19 August 2021. Access Date: 24 September 2021. https://www.meti.go.jp/english/press/2021/0819_002.html

[2203] FSC to Introduce Routine Inspection of Personal Data Protection at Financial Institutions, Financial Services Commission (Seoul) 07 December 2020. Access Date: 17 May 2021. https://www.fsc.go.kr/eng/pr010101/22547

[2204] 2021 Action Plan for Digital New Deal, Ministry of Science and ICT (Seoul) 25 February 2021. Access Date: 13 April 2021. https://english.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=2&bbsSeqNo=42&nttSeqNo=483&searchOpt=ALL&searchTxt=

thousand future researchers in promising areas such as Artificial Intelligence technologies, biotechnologies and renewables.[2205]

On 23 March 2021, Secretary of Planning and Policies of Science, Technology and Innovation Diego Hurtado representing Argentina's Ministry of Science, Technology and Innovation, participated in the 2021 Korea-Latin America Digital Cooperation Forum whose central theme was the "Association for the Innovation and Digital Inclusion" organized by Korea's Ministry of Foreign Affairs. Secretary Hurtado celebrated the organization of this forum, the purpose of which is to consolidate efforts to share experiences in the face of digital transformation and promote Korea-Latin America cooperation in the areas of digital infrastructure, digital government, smart city and cybersecurity.[2206]

On 7 April 2021, Minister of Foreign Affairs Eui-Yong Chung invited Mexico's National Digital Strategy Coordination of Mexico to participate virtually in the 2021 Korea-Latin America Digital Cooperation Forum. The head of the National Digital Strategy Coordination Carlos Emiliano Calderón Mercado "highlighted the importance of digital sovereignty for information security, since each country must maintain control of its technological operation and strengthen technical measures to reduce cybersecurity risks, under a continuous improvement model. Likewise, he explained that technological autonomy offers countries the opportunity to define the training areas for their public servants, as well as the possibility of implementing focused strategies and tools compatible with the infrastructure, the reuse of source code and a greater use of standards. open. He pointed out that information security management implies carrying out institutional evaluations to make a timely detection of vulnerabilities, mitigate risks against possible threats and coordinate between institutions, the implementation of a protocol for incident management. cybernetics, with the aim of standardizing the actions of identification, protection, detection, response and recovery of information in the event of a cybersecurity incident."[2207]

On 13 May 2021, the Ministry of Science and Technology presented the Strategy to realize trustworthy artificial intelligence. The Strategy will be implemented step by step until 2025. Among the Strategy's goals – "set the criteria for high-risk artificial intelligence which may pose a potential threat to the citizens" safety or basic rights and make service providers "notify" users of whether the risky artificial intelligence will be used.'[2208]

Korea has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, Korea receives a score of +1.

Analyst: Alexander Ignatov

[2205] Establish the 4th Basic Plan for Nurturing and Supporting Scientific Talents (2021 – 2025), Ministry of Science and ICT (Seoul) 30 March 2021. Access Date: 13 April 2021. https://english.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=490&searchOpt=ALL&searchTxt=

[2206] Argentina participó del Foro de Cooperación Digital Corea-Latinoamérica 2021, Government of Argentina 23 March 2021. Access Date: 13 May 2021. https://www.argentina.gob.ar/noticias/argentina-participo-del-foro-de-cooperacion-digital-corea-latinoamerica-2021

[2207] Soberanía digital, estrategia clave para la seguridad de la información, plantea la CEDN ante Ministerios de TIC de Corea y Latinoamérica [Digital sovereignty, a key strategy for information security, raises the CEDN before ICT Ministries of Korea and Latin America], Mexican Government (Mexico City) 7 April 2021. Translation provided by Google Translate. Access Date: 13 May 2021. https://www.gob.mx/cedn/es/articulos/soberania-digital-estrategia-clave-para-la-seguridad-de-la-informacion-plantea-la-cedn-ante-ministerios-de-tic-de-corea-y-latinoamerica

[2208] MSIT announced Strategy to realize trustworthy artificial intelligence, the Ministry of Science and ICT of the Republic of Korea (Sejong-Si) 13 May 2021. Access Date: 27 September 2021. https://english.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=509&searchOpt=ALL&searchTxt=

Mexico: +1

Mexico has fully complied with the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 19 January 2021, "the Tax Administration Service (SAT) reiterated its commitment to taxpayers to safeguard their confidential information, which is provided when they carry out procedures on the Portal with the use of the Password or the e.signature."[2209] The SAT constantly carries out "actions to identify situations that put taxpayers' operations at risk: Identifies atypical behaviors in the issuance of invoices; sends messages through the Tax Mailbox informing about operations that need to be corrected in order to avoid fines or other more severe measures; disables passwords at risk or passwords of taxpayers who have been reported by the health and public registry authorities as deceased to avoid identity theft and the improper use of their data."[2210]

On 25 January 2021, "in order to reduce risk situations for students and teachers as Internet users, in addition to contributing to making girls, boys, adolescents and young people less vulnerable to harmful content of the digital age, the National College of Technical Professional Education and Microsoft, presented the e-Book Digital Security Essentials…This joint action seeks to generate in the student community a culture of digital coexistence, raise awareness about habits and behaviors in risk situations, as well as good practices, in addition to helping to protect privacy, increase security and teach how to be a good digital citizen."[2211]

On 25 March 2021, General Guidelines for the Protection of Personal Data for the Public Sector entered into force. It obligated subjects to enable on its institutional Internet portal, a section called "Protection of Personal Data."[2212]

On 7 April 2021, Carlos Emiliano Calderón Mercado, head of the National Digital Strategy Co-ordination, was invited by Korea's Minister of Foreign Affairs Eui-Yong Chung to participate virtually in the 2021 Korea-Latin America Digital Cooperation Forum. He "highlighted the importance of digital sovereignty for information security, since each country must maintain control of its technological operation and strengthen technical measures to reduce cybersecurity risks, under a continuous improvement model. Likewise, he explained that technological autonomy offers countries the opportunity to define the training areas for their public servants, as well as the possibility of implementing focused strategies and tools compatible with the infrastructure, the reuse of source code and a greater use of standards. open. He pointed out that information security management implies carrying out institutional evaluations to make a timely detection of vulnerabilities, mitigate risks against possible threats and coordinate between institutions, the implementation of a protocol for incident management. cybernetics, with the aim of standardizing

[2209] Seguridad y protección de datos del contribuyente [Taxpayer data security and protection], Mexican Government (Mexico City) 19 January 2021. Translation provided by Google Translate. Access Date: 13 May 2021. https://www.gob.mx/sat/prensa/seguridad-y-proteccion-de-datos-del-contribuyente-011-2021

[2210] Seguridad y protección de datos del contribuyente [Taxpayer data security and protection], Mexican Government (Mexico City) 19 January 2021. Translation provided by Google Translate. Access Date: 13 May 2021. https://www.gob.mx/sat/prensa/seguridad-y-proteccion-de-datos-del-contribuyente-011-2021

[2211] Boletín SEP no. 20 Fortalece CONALEP la formación de alumnos y profesores con una nueva herramienta para fomentar la Seguridad Digital [SEP Bulletin no. 20 CONALEP strengthens the training of students and teachers with a new tool to promote Digital Security], Mexican Government (Mexico City) 25 January 2021. Translation provided by Google Translate. Access Date: 13 May 2021. https://www.gob.mx/sep/es/articulos/boletin-sep-no-20-fortalece-conalep-la-formacion-de-alumnos-y-profesores-con-una-nueva-herramienta-para-fomentar-la-seguridad-digital

[2212] Personal data protection, Mexican Government (Mexico City) 25 March 2021. Access Date: 13 May 2021. https://www.gob.mx/salud/cenetec/acciones-y-programas/proteccion-de-datos-personales-267758

the actions of identification, protection, detection, response and recovery of information in the event of a cybersecurity incident."[2213]

On 23 April 2021, Cyber Incident Response Center of the National Guard's Scientific Directorate issued Responsible digital identity recommendations. It explained what information can be stolen, what situations are the riskiest and gave advice on how to protect the data and what to do in case of fraud.[2214]

On 3 May 2021, Federal Consumer Prosecutor's Office issued the Code of Ethics in Electronic Commerce. It is a set of values and principles that all member suppliers must observe in activities related to electronic commerce, in order to: respect and promote the rights of the consumer population, promote a culture of responsible consumption, promote human rights of consumers, promote ethical and responsible digital advertising, protect vulnerable groups, encourage self-regulation.[2215]

On 1 September 2021, Federal Consumer Prosecutor's Office launched the call for suppliers of goods, products or services to participate in obtaining of the Profeco Digital Distinction, for promoting and strengthening security, transparency and confidentiality in electronic commerce. The recognition will be granted to those providers that stand out for providing the consumer with the proper information, greater reliability and legal certainty in transactions through the use of electronic, optical or any other technology.[2216]

Mexico has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, Mexico receives a score of +1.

Analyst: Irina Popova

Russia: +1

Russia has fully complied with the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 28 December 2020, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation promulgated the Order No. 777 "On Implementation of Recommendations on Certification of Communication Devices Used in Public Access Networks Allowing Functioning

[2213] Soberanía digital, estrategia clave para la seguridad de la información, plantea la CEDN ante Ministerios de TIC de Corea y Latinoamérica [Digital sovereignty, a key strategy for information security, raises the CEDN before ICT Ministries of Korea and Latin America], Mexican Government (Mexico City) 7 April 2021. Translation provided by Google Translate. Access Date: 13 May 2021. https://www.gob.mx/cedn/es/articulos/soberania-digital-estrategia-clave-para-la-seguridad-de-la-informacion-plantea-la-cedn-ante-ministerios-de-tic-de-corea-y-latinoamerica

[2214] Identidad digital responsible [Responsible digital identity], Mexican Government (Mexico City) 23 April 2021. Access Date: 13 May 2021. https://www.gob.mx/gncertmx/articulos/105224

[2215] Código de Ética en materia de Comercio Electrónico [Code of Ethics in Electronic Commerce], Mexican Government (Mexico City) 3 May 2021. Access Date: 13 May 2021. https://www.gob.mx/profeco/es/articulos/codigo-de-etica-en-materia-de-comercio-electronico

[2216] Profeco launches call for suppliers to obtain Digital Badge, Government of Mexico (Mexico City) 1 September 2021. Translation provided by Google Translate. Access Date: 21 September 2021. https://www.gob.mx/profeco/prensa/lanza-profeco-convocatoria-a-proveedores-para-obtener-distintivo-digital?idiom=es

of Important Objects of Critical Information Infrastructure."[2217] The Recommendations are a restricted circulation document that has never been presented for public discussion.

On 28 December 2020, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation promulgated the Order No. 779 "On Technical and Organizational Measures to Promote Information Security of Public Access Networks Allowing Functioning of Important Objects of Critical Information Infrastructure."[2218]

On 28 December 2020, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation promulgated the Order No.780 "On Detecting Threats to Stability, Security and Integrity of the Internet and public access networks in the Russian Federation."[2219] The list of threat to stability, security and integrity of information networks in Russia hasn't been presented for public consideration.

On 15 February 2021, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation declared starting of the federal project "Cadres for the Digital Economy" aimed at wider spread of digital skills among administrative personnel, governmental officials and education specialists.[2220]

On 18 February 2021, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation initiated the "KLIK" program that is designed to facilitate digital transformation of Russia's economy by wider spread of digital skills, especially data-related competencies. Vice Minister Eugeney Kislyakov said that the program would contribute to further improvement of the effectiveness of business and government bodies' performance.[2221]

On 3 March 2021, the Ministry Digital Development, Communications and Mass Media of the Russian Federation presented amendments to the Federal Law "On Personal Data." The Ministry proposed to introduce several restrictions on personal data operators to limit their capability to identify an information owner with exceptions implying threats to a subject's health and security.[2222]

On 12 May 2021, the Ministry Digital Development, Communications and Mass Media of the Russian Federation and the Internet Initiatives Development Fund launched a joint initiative to accelerate development of Russian IT start-ups. The program is designed to promote skills and

[2217] Order №777 "On Implementation of Recommendations on Certification of Communication Devices Used in Public Access Networks Allowing Functioning of Important Objects of Critical Information Infrastructure," Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Moscow) 28 December 2020. Access Date: 29 March 2021. https://digital.gov.ru/ru/documents/7446/

[2218] Order №789 "On Technical and Organizational Measures to Promote Information Security of Public Access Networks Allowing Functioning of Important Objects of Critical Information Infrastructure," Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Moscow) 28 December 2020. Access Date: 29 March 2021. https://digital.gov.ru/ru/documents/7442/

[2219] Order №780 "On Detecting Threats to Stability, Security and Integrity of the Internet and public access networks in the Russian Federation,', Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Moscow) 28 December 2020. Access Date: 29 March 2021. https://digital.gov.ru/ru/documents/7450/

[2220] Start of the "Digital Economy" educational program, Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Moscow) 15 February 2021. Access Date: 29 March 2021. https://digital.gov.ru/ru/events/40374/

[2221] Selection for Digital Economy Training Started, Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Moscow) 18 February 2021. Access Date: 29 March 2021. https://digital.gov.ru/ru/events/40394/

[2222] Ministry of Digital Development of Russia to Discuss Amendments to the Federal Law "On Personal Data," Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Moscow) 3 March 2021. Access Date: 17 May 2021. https://digital.gov.ru/ru/events/40498/

competencies development among information technology entrepreneurs along with boosting start-ups investment attractiveness.[2223]

On 27 July 2021, the Ministry of Digital Development announced the launch of a new digital education platform "Gotov k Cifre" ("Ready for Digital"). The platform will aggregate digital educational resources to facilitate spread of digital skills and competences.[2224]

On 14 September 2021, Russia approved the set of measures to facilitate the national IT industry. These measures are designed to promote demand on Russia-made digital solutions, accelerate the digital transformation and create open environment for IT-businesses. The package includes 62 measures that involve lifting of legal restrictions on implementation of cut-edge solutions and new digital standards, financial support for establishment of new national digital platforms and training of personnel.[2225]

Russia has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, Russia receives a score of +1.

Analyst: Alexander Ignatov

Saudi Arabia: +1

Saudi Arabia has fully complied with the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 30 December 2020, Saudi Arabia approved the launch of new digital economy policy to encourage investment, accelerate local technical leadership and to attract international partnerships based on transfer of expertise and cooperation in the field of innovation and technical and digital transformation.[2226]

On 10 March 2021, Saudi Arabia approved the establishment of the Digital Government Authority. The Authority is tasked with preparing the national eGovernment strategy; overseeing digital government platforms, websites, services and networks; establishing technical standards for government digital transformation models; and regulating Saudi Arabia's government cloud. The launch of the Authority is expected to further accelerate digital transformation and the provision of e-government services in the Kingdom.[2227]

On 30 May 2021, the Communications and Information Technology Commission announced the implementation of a regulatory framework to beef up cybersecurity in Saudi Arabia. The

[2223] Ministry of Digital Development of Russia Invites Russian IT Strat-Ups to Participate in Acceleration Program, Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Moscow) 12 May 2021. Access Date: 17 May 2021. https://digital.gov.ru/ru/events/40934/

[2224] A New Online Service "Ready for Digital" Launched in Russia, the Ministry of Digital Development of the Russian Federation (Moscow) 27 July 2021. Translation provided by the analyst. Access Date: 22 September 2021. https://digital.gov.ru/ru/events/41195/

[2225] The Government approved the second package for promotion of IT-industries, the Government of the Russian Federation (Moscow) 14 September 2021. Translation provided by the analyst. Access Date: 22 September 2021. http://government.ru/news/43255/

[2226] Saudi Arabia launches digital economy policy to become competitive, diversify, Saudi Gazette (Riyadh) 30 December 2020. Access Date: 30 April 2021. https://www.saudigazette.com.sa/article/601959

[2227] Access Alert: Saudi Arabia's New Digital Government Authority, Access Partnership (Riyadh) 11 March 2021. Access Date: 30 April 2021. https://www.accesspartnership.com/access-alert-ksas-new-digital-government-authority/

"cybersecurity regulatory framework" for service providers in the communications, IT, and postal services sector aims to raise the security levels of service providers. It seeks to ensure the implementation of adequate cybersecurity measures compliant with the best international practices.[2228]

On 6 August 2021, it was reported that Minister of Communications and Information Technology Abdullah Alswaha, during his speech to the G20 digital economy ministers' meeting, said that Saudi Arabia topped the list of leading countries in the digital economy. According to minister, NEOM City, the largest global platform for innovators, is an ideal example of harmonizing regulation and innovation, to achieve well-being through the adaptation of technology and innovation.[2229]

On 15 September 2021, the Council of Ministers of Saudi Arabia approved the Personal Data Protection Law, which will take effect on 13 March 2022. In a statement, Saudi Data and AI Authority President Abdullah bin Sharaf Alghamdi said the law would accelerate Saudi Arabia's digitization efforts while helping to create an information-based society. The law protects the rights related to processing personal data, regulates their sharing between entities, and prevents their misuse, and will therefore enhance the local economy and build trust in the data sector.[2230]

Saudi Arabia has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, Saudi Arabia receives a score of +1.

Analyst: Pavel Doronin

South Africa: 0

South Africa has partially complied with the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 19 January 2021, South Africa launched a new educational program for public servants to promote digital skills. Another aim of the program is to teach public officials necessary crisis management and leadership skills. The program is a joint venture in partnership with the Ecole Nationale d'Administration of France.[2231]

On 25 February 2021, the National Treasury announced allocation of ZAR217 billion (approximately USD14 billion) to promote economic growth. The sum is said to be spent over the next three years. Over the medium term, ZAR5.3 billion (approximately USD3.6 billion) would be set aside for the Department of Science and Innovation to scale up interventions supporting the local production of

[2228] Saudi Arabia implements cybersecurity framework, The Arab News (Riyadh) 30 May 2021. Access Date: 24 September 2021. https://www.arabnews.com/node/1867196/business-economy

[2229] Saudi Arabia leads in global digital economy, minister says, the Arab News (Riyadh) 6 August 2021. Access Date: 24 September 2021. https://www.arabnews.com/node/1906631/business-economy

[2230] Saudi Arabia approves law to protect personal data, India TV (Riyadh) 15 September 2021. Access Date: 24 September 2021. https://www.indiatvnews.com/news/world/saudi-arabia-approves-law-protect-personal-data-latest-international-news-updates-734006

[2231] Public servants to get training on digital transformation, South African Government News Agency (Pretoria) 19 January 2021. Access Date: 13 April 2021. https://www.sanews.gov.za/south-africa/public-servants-get-training-digital-transformation

ventilators, nano satellites, hydrogen fuel cell technologies, and renewable energy research development and pilots.[2232]

On 25 February 2021, President Cyril Ramaphosa announced that the Department of Basic Education had submitted amendments to the national school curriculum. Some schools in South Africa were said to incorporate the new coding and robotics curriculum in 2021. The new curriculum was submitted for consideration by the Council for Quality Assurance in General and Further Education and Training.[2233]

On 11 March 2021, South Africa decided to relocate extra funds to fulfil the obligations under the National Student Financial Aid Scheme. Further reprioritization is considered as a part of the Medium-Term Budget process that would take place later this year.[2234]

On 15 June 2021, the Government Communication and Information System and the Ministry of Communication and Digital Technologies hosted a masterclass on digital skills development for the youth. Representatives of the governmental authorities and private entities including Google joined to younger generations for the fast-changing technological landscape.[2235]

South Africa takes steps to promote digital security and empower consumers by means of skills development. However, no actions aimed at fostering open, fair, and non-discriminatory have been founded within the monitoring period.

Thus, South Africa receives a score of 0.

Analyst: Alexander Ignatov

Turkey: +1

Turkey has fully complied with the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 4 December 2020, Regulation 31324 on the Processing of Personal Data and Protection of Privacy in the Electronic Communication Sector was published in the Official Gazette; the Regulation has been developed in accordance with the general personal data protection rules established in the Electronic Communication Law and the Personal Data Protection Law, and is aimed to ensure the protection and privacy of personal data in the communications sector and the regulation of procedures and principles regarding operators' relevant data protection obligations. The Regulation defines the minimum technical and administrative measures that must be taken by operators to ensure the safety of their services and personal data, including establishing required security policies; protection of personal data against data breaches such as unauthorized or unlawful access to, or the damage, loss, or disclosure of such data; ensuring the security of systems storing

[2232] R217 billion allocated for economic growth programmes, South African Government News Agency (Pretoria) 25 February 2021. Access Date: 13 April 2021. https://www.sanews.gov.za/south-africa/r217-billion-allocated-economic-growth-programmes

[2233] Some schools to start piloting coding, robotics curriculum, South African Government News Agency (Pretoria) 25 February 2021. Access Date: 13 April 2021. https://www.sanews.gov.za/south-africa/some-schools-start-piloting-coding-robotics-curriculum

[2234] NSFAS to release funds for new qualifying students, South African Government News Agency (Pretoria) 11 March 2021. Access Date: 13 April 2021. https://www.sanews.gov.za/south-africa/nsfas-release-funds-new-qualifying-students

[2235] Government hosts Youth Masterclass on Digital Skills Development Opportunities, 15 Jun, South African Government (Pretoria) 11 June 2021. Access Date: 23 August 2021. https://www.gov.za/speeches/government-hosts-youth-masterclass-digital-skills-development-opportunities-25-jun-11-jun

personal data. The Regulation further clarifies the procedures and principles that apply to the obligation to obtain consent.[2236]

On 22 December 2020, the Data Protection Authority published a new decision, numbered 2020/966, which highlights the importance of the general principles that personal data processed must be accurate and up-to-date. The Decision emphasizes that the data controller has an active duty of care and that it is crucial to verify that personal data is accurate and up to date. The Decision states that in order to ensure the accuracy and timeliness of the data, the channels for collecting personal data must be clearly defined. In addition, reasonable measures must be taken, such as checking through verification codes, to avoid harm to the data owner due to the inaccuracy of personal data.[2237]

On 30 December 2020, it was reported that President Recep Tayyip Erdoğan signed the country's new national cyber security plan (2020-2023) prepared by Turkey's Transport and Infrastructure Ministry in coordination with the non-governmental organizations, universities, public and private sectors; Turkey's National Cyber Security Strategy and Action Plan include 40 actions and 75 implementation steps in relation to strategic objectives, including to protect the cybersecurity of critical infrastructure, to develop national technological tools for operational needs and to enhance the competencies of teams fighting cyber threats.[2238]

On 12 January 2021, it was reported that the Data Protection Authority launched an investigation into WhatsApp over its new data-sharing rules (sharing of more personal data with Facebook), while the Competition Authority opened a probe into Facebook and WhatsApp and suspended the messenger's new data collection rules in the country. The investigations will look into such issues, as general compliance with personal data protection legislation, data processing conditions and data transfer abroad.[2239]

On 12 March 2021, Turkey unveiled the details of a major new economic reform package as pledged by the president last November; as a part of the reform a digital tax office will be established which will operate 24 hours a day, seven days a week to enable the public to carry out transactions in the digital environment without personally visiting a tax office.[2240]

On 15 March 2021, it was reported that Turkey promoted the establishment of a "cyber security cluster," made up of local companies that produce software and hardware, aiming to make indigenous products dominant in the country; the cluster currently comprises 180 Turkish companies.[2241]

[2236] The Regulation on the Processing of Personal Data and Protection of Privacy in the Electronic Communication Sector Published | Turkey, ICLG (Ankara) 9 December 2020. Access Date: 10 May 2021. https://iclg.com/briefing/15242-the-regulation-on-the-processing-of-personal-data-and-protection-of-privacy-in-the-electronic-communication-sector-published-turkey

[2237] Turkey: New decision of the Turkish Data Protection Authority, Lexology (London) 3 March 2021. Access Date: 10 May 2021. https://www.lexology.com/library/detail.aspx?g=9add5710-ca4f-445a-93c7-ff73c73a913e

[2238] Turkey reveals its three-year cybersecurity plan, TRT World (Istanbul) 30 December 2020. Access Date: 10 May 2021. https://www.trtworld.com/magazine/turkey-reveals-its-three-year-cybersecurity-plan-42820

[2239] Turkish watchdog opens WhatsApp probe over new rules, Anadolu Agency (Ankara) 12 January 2021. Access Date: 10 May 2021. https://www.aa.com.tr/en/science-technology/turkish-watchdog-opens-whatsapp-probe-over-new-rules/2107212

[2240] Turkey announces landmark new economic reform package, Anadolu Agency (Ankara) 12 March 2021. Access Date: 30 April 2021. https://www.aa.com.tr/en/economy/turkey-announces-landmark-new-economic-reform-package/2173910

[2241] Turkey promotes indigenous 'Cyber Security Cluster': Defense industries head, Hurriyet (Ankara) 15 March 2021. Access Date: 10 May 2021. https://www.hurriyetdailynews.com/turkey-promotes-indigenous-cyber-security-cluster-defense-industries-head-163129

On 5 April 2021, it was reported that Turkish Data Protection Authority launched a direct investigation into Facebook over a user data leak.[2242]

On 21 June 2021, the Personal Data Protection Authority published a summary of its decision 2021/426, dated 27 April 2021, in which it fined a software company TRY400,000 (approx. EUR38,695) for data security and breach notification failures under the Law on Protection of Personal Data No. 6698. In particular, it was highlighted that the company had failed to take the necessary technical and administrative measures pursuant to Article 12(1) of the Law and failed to notify the Authority within the prescribed time frame pursuant to Article 12(5) of the Law.[2243]

On 10 August 2021, it was reported that in July 2021, the Turkish Personal Data Protection Board published nine decisions and announced five data breach notifications. The insurance industry came under particular scrutiny, as four of the nine published decisions relate to insurance companies. Another important data protection development in July was the publication in the Official Gazette of the Constitutional Court's decision on an individual application regarding the right to request the protection of personal data.[2244]

On 3 September 2021, the Personal Data Protection Authority fined WhatsApp nearly EUR200,000 for violating privacy rules. The Facebook-owned messaging platform had "not clearly stated" how it would process its users' data and for what purpose. The Authority ordered the app to bring its privacy policy in line with Turkey's laws.[2245]

On 14 September 2021, the Ministry of Transport, Communications and High Technologies of Azerbaijan held a meeting with a delegation headed by the Chairman of the Digital Transformation Office of the Turkish Presidential Administration, Ali Taha Koc. Issues of implementing the concept of digital transformation of Azerbaijan, cybersecurity, personal data protection, the "government cloud", as well as other issues of upcoming cooperation were discussed. The "Roadmap of the Azerbaijani-Turkish Working Group on Digital Transformation between the Ministry of Transport, Communications and High Technologies of Azerbaijan and the Digital Transformation Office of the Turkish Presidential Administration" was signed.[2246]

Turkey has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, Turkey receives a score of +1.

Analyst: Pavel Doronin

[2242] Turkey launches probe into Facebook over data leak, Hurriyet (Ankara) 5 April 2021. Access Date: 10 May 2021. https://www.hurriyetdailynews.com/turkey-launches-probe-into-facebook-over-data-leak-163708
[2243] Turkey: KVKK fines software company TL 400,000 for data breach, DataGuidlines (Atlanta) 22 June 2021. Access Date: 24 September 2021. https://www.dataguidance.com/news/turkey-kvkk-fines-software-company-tl-400000-data
[2244] Turkey: Two-minute Recap Of Recent Developments In Turkish Personal Data Protection Law – July 2021, Mondaq (New York) 10 August 2021. Access Date: 24 September 2021. https://www.mondaq.com/turkey/data-protection/1100144/two-minute-recap-of-recent-developments-in-turkish-personal-data-protection-law-july-2021
[2245] Turkey fines WhatsApp €197,000 over controversial privacy update, Euronews (Lyon) 3 September 2021. Access Date: 24 September 2021. https://www.euronews.com/2021/09/03/turkey-fines-whatsapp-197-000-over-controversial-privacy-update
[2246] Azerbaijani-Turkish Working Group develop roadmap on digital transformation, Turkic World (Antalya) 14 September 2021. Access Date: 24 September 2021. https://turkic.world/en/articles/economy/12807

United Kingdom: +1

The United Kingdom has fully complied with the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

On 16 March 2021, the UK published the Integrated Review of Security, Defence, Development and Foreign Policy. It stated the bearing of new capabilities for the National Cyber Force. Learning from the pandemic, it bolstered national resilience with a new Situation Centre at the heart of government, improving use of data and the ability to anticipate and respond to future crises.[2247]

On 30 April 2021, the Foreign, Commonwealth and Development Office published the UK/EU and Eurasian Economic Community: Trade and Cooperation Agreement, there were fixed the existing levels of liberalisation in UK and EU markets, confirming both sides' leadership in this area and commitment to openness, as well as obligations on net neutrality, which fulfilled the UK's dual aims of securing commitments towards an open internet and protecting the safety of users online.[2248]

On 10 May 2021, the fourth annual report on the National Cyber Security Centre's Active Cyber Defence programme was released. It disclosed it had taken down more scams in the last year than in the previous three years combined as the organization moved to further protect the UK public and critical services such as the National Health Service during the COVID-19 pandemic.[2249]

The United Kingdom has taken actions in all three aspects of the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

Thus, the United Kingdom receives a score of +1.

Analyst: Sergei Vasilkovsky

United States: 0

United States has partially complied with the commitment to foster an open, fair, and non-discriminatory environment, protect and empowering consumers, and address the challenges related to privacy, data protection, intellectual property rights, and security.

On 14 December 2020, the Federal Trade Commission, in cooperation with 19 federal, state, and local law enforcement partners announced a "nationwide crackdown on scams that target consumers with fake promises of income and financial independence that have no basis in reality," nicknamed "Operation Income Illusion." The crackdown encompassed more than 50 law enforcement actions

[2247] Integrated Review sets vision for stronger, more secure, prosperous and resilient nation, Government of the United Kingdom (London) 16 March 2021. Access Date: 14 May 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf
[2248] UK/EU and EAEC: Trade and Cooperation Agreement [TS No.8/2021], Government of the United Kingdom (London) 30 April 2021. Access Date: 14 May 2021. https://www.gov.uk/government/publications/agreements-reached-between-the-united-kingdom-of-great-britain-and-northern-ireland-and-the-european-union/summary-explainer
[2249] Active Cyber Defence – The fourth Year, the National Cyber Security Centre (London) 10 May 2021. Access Date: 14 May 2021. https://www.ncsc.gov.uk/files/Active-Cyber-Defence-ACD-The-Fourth-Year.pdf

targeting work-from-home and employment scams, pyramid schemes, investment scams, bogus coaching courses, and other schemes.[2250]

On 3 February 2021, the Federal Trade Commission announced that it had sent refunds totaling around USD4.7 million to 10,249 victims of the Digital Altitude business coaching scheme.[2251]

On 22 February 2021, the Department of Homeland Security Science and Technology Directorate and the Cybersecurity and Infrastructure Security Agency announced seven grant awards to the Secure and Resilient Mobile Network Infrastructure project. The awards, totaling USD9.75 million, were aimed at "developing protections for legacy cellular networks — 2G, 3G and 4G, building security into the newly launched 5G network, and developing end-to-end protection of network traffic, including a standardized secure voice capability for unclassified government communications."[2252]

On 8 March 2021, the Department of Homeland Security Science and Technology Directorate and the Cybersecurity and Infrastructure Security Agency announced two additional grant awards to the Secure and Resilient Mobile Network Infrastructure project. The two awards, USD915,000 and USD1.2 million, respectively, are focused on developing solutions designed to "improve the government's visibility into mobile device network traffic to identify malware, attacks or attempts to extract data from or through mobile devices."[2253]

On 12 May 2021, President Joseph Biden signed the Executive Order on Improving the Nation's Cybersecurity. The Order aims to: remove barriers to threat information sharing between government and the private sector; modernize and implement stronger cybersecurity standards in the federal government; improve software supply chain security; establish a cybersecurity safety review board; create a standard playbook for responding to cyber incidents; improve detection of cybersecurity incidents on federal government networks; and improve investigative and remediation capabilities.[2254]

The United States has taken actions in two of the three issue areas related to digital growth: empowering and protecting consumers while addressing issues related to privacy, data protection and intellectual property rights; and addressing digital security risks.

Thus, the United States receives a score of 0.

Analyst: Andrei Sakharov

[2250] As Scammers Leverage Pandemic Fears, FTC and Law Enforcement Partners Crack Down on Deceptive Income Schemes Nationwide, Federal Trade Commission (Washington, DC) 14 December 2020. Access Date: 15 May 2021. https://www.ftc.gov/news-events/press-releases/2020/12/scammers-leverage-pandemic-fears-ftc-law-enforcement-partners

[2251] FTC Sends Nearly $4.7 Million to Victims of Digital Altitude Business Coaching Scheme, Federal Trade Commission (Washington, DC) 3 February 2021. Access Date: 15 May 2021. https://www.ftc.gov/news-events/press-releases/2021/02/ftc-sends-nearly-47-million-victims-digital-altitude-business

[2252] News Release: DHS Announces Seven R&D Awards to Help Secure Nation's Mobile Network Infrastructure, Department of Homeland Security (Washington, DC) 8 March 2021. Access Date: 15 May 2021. https://www.dhs.gov/science-and-technology/news/2021/02/22/news-release-dhs-announces-rd-awards-help-secure-mobile-network-infrastructure#

[2253] News Release: DHS Announces Two R&D Projects to Enhance Mobile Network Traffic Security, Department of Homeland Security (Washington, DC) 8 March 2021. Access Date: 15 May 2021. https://www.dhs.gov/science-and-technology/news/2021/03/08/news-release-dhs-announces-two-rd-projects-enhance-mobile-network-traffic-security

[2254] Executive Order on Improving the Nation's Cybersecurity, the White House (Washington, DC) 12 May 2021. Access Date: 15 May 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

European Union: +1

The European Union has fully complied with the commitment to support fostering an open, fair, and non-discriminatory environment, and protecting and empowering consumers, while addressing the challenges related to privacy, data protection, intellectual property rights, and security.

In December 2020, the European Commission proposed the Digital Services Act and the Digital Markets Act. One of the main goals of the two initiatives is to create a safer digital environment and ensure the fundamental rights of all users of digital services are protected. The Acts include a set of rules to improve consumer safety across online platforms in the EU, including online marketplaces, to make consumers equally safe when shopping online or offline. Platforms are obliged to step up efforts to tackle traders selling fake or unsafe products and to stop fraudulent companies using their services.[2255]

On 16 December 2020, was adopted the new EU's Cybersecurity Strategy in the Digital Decade. It stated that the EU should boost the security of essential services and strength collective capabilities and international stability in cyberspace.[2256]

On 2 March 2021, the Agency for Cybersecurity and the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies announced the signature of a memorandum of understanding to enhance the cybersecurity.[2257]

On 23 April 2021, the European Union's lead data protection supervisor called for remote biometric surveillance in public places to be banned outright under incoming AI legislation.[2258]

On 12 May 2021, the Commission proposed new rules and actions aiming to turn Europe into the global hub for trustworthy Artificial Intelligence (AI). The combination of the first-ever legal framework on AI and a new Coordinated Plan with Member States would guarantee the safety and fundamental rights of people and businesses, while strengthening AI uptake, investment and innovation across the EU.[2259]

On 12 May 2021, the European Commission launched a public consultation on the formulation of a set of principles to promote and uphold EU values in the digital space. These principles aimed to guide the EU and Member States in designing digital rules and regulations that deliver the benefits of digitalisation for all citizens.[2260]

The EU has taken strong actions that match all three areas: fostering open, fair, and non-discriminatory environment; empowering and protecting consumers while addressing issues related to privacy, data protection and intellectual property rights; and addressing digital security risks.

Thus, the European Union receives a score of +1.

Analysts: Sergei Vasilkovsky and Andrey Shelepov

[2255] The Digital Services Act package, European Commission (Brussels) December 2020. Access Date: 27 September 2021. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[2256] The EU's Cybersecurity Strategy in the Digital Decade (Brussels) 16 December 2021. Access Date: 14 May 2021. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade
[2257] ENISA and CERT-EU sign Agreement to start their Structured Cooperation (Brussels) 2 March 2021. Access Date: 14 May 2021. https://www.enisa.europa.eu/news/enisa-news/enisa-and-cert-eu-sign-agreement-to-start-their-structured-cooperation
[2258] EU's top data protection supervisor urges ban on facial recognition in public (Brussels) 23 April 2021. Access Date: 14 May 2021. https://techcrunch.com/2021/04/23/eus-top-data-protection-supervisor-urges-ban-on-facial-recognition-in-public
[2259] Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence (Brussels) 12 May 2021. Access Date: 14 May 2021. https://digital-strategy.ec.europa.eu/en/news/europe-fit-digital-age-commission-proposes-new-rules-and-actions-excellence-and-trust-artificial
[2260] Europe's Digital Decade: Commission launches consultation and discussion on EU digital principles (Brussels) 12 May 2021. Access Date: 14 May 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2288