2021 G20 Rome Summit Interim Compliance Report

Prepared by
Kaylin Dawe, Sonja Dobson 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 1 November 2021 to 22 June 2022

16 September 2022

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

University of Toronto
1 Devonshire Place
North House, Room 209
Toronto, Ontario M5S 3K7
Canada
www.g20.utoronto.ca

G20 RESEARCH GROUP
@g20rg

Centre for International Institutions Research at
the Russian Presidential Academy of National
Economy and Public Administration
11 Prechistenskaya nabarezhnaya
Moscow, Russia 119034
www.ranepa.ru/eng/ciir

4. Digital Economy: Challenges

"We will continue to work on addressing challenges such as those related to privacy, data protection, security and intellectual property rights, in accordance with the relevant applicable legal frameworks."

G20 Rome Leaders' Declaration

Assessment

	No Compliance	Partial Compliance	Full Compliance
Argentina		0	
Australia		0	
Brazil			+1
Canada			+1
China			+1
France		0	
Germany			+1
India			+1
Indonesia		0	
Italy			+1
Japan			+1
Korea			+1
Mexico			+1
Russia		0	
Saudi Arabia		0	
South Africa		0	
Turkey		0	
United Kingdom			+1
United States			+1
European Union			+1
Average	+0.60 (80%)		

Background

The G20 addressed the issues related to digital growth for the first time at the 2015 Antalya Summit, 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."[475] 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. The 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).[476]

At the 2016 Hangzhou Summit, 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 optimization."[477] The leaders pledged to

[475] Adjusted Growth Strategy: Germany, RANEPA (Moscow) 2015. Access Date: 11 January 2022. https://www.ranepa.ru/images/media/g20/2015Antalya/Adjusted-Growth-Strategy-2015-Germany.pdf

[476] G20 Leaders' Communique Antalya Summit, RANEPA (Moscow) 16 November 2015. Access Date: 11 January 2022. https://www.ranepa.ru/images/media/g20/2015Antalya/000111117.pdf

[477] G20 Blueprint on Innovative Growth, RANEPA (Moscow) 05 September 2016. Access Date: 11 January 2022. https://www.ranepa.ru/images/media/g20/2016Hangzhou/G20%20Blueprint%20on%20Innovative%20Growth.pdf

"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." To facilitate "the G20 agenda on innovation, new industrial revolution and digital economy,"[478] G20 leaders decided to establish a designated task force supported by the Organisation for Economic Co-operation and Development (OECD).

At the 2017 Hamburg Summit, the G20 addressed the issue of digital skills promotion. The #eSkills4Girls Initiative touched on the issue within the broader context of development and gender policy.[479] To facilitate implementing commitments on digital growth, the Digital Economy Task Force (DETF) was established following the decision made at the 2016 Hangzhou Summit. 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. During Argentina's G20 presidency in 2018, the DETF presented political tools for digital growth including the G20 Digital Governance Principles, recommendations for measuring the digital economy, gender equality in digital sphere and digital infrastructure development.

At the 2018 Buenos Aires Summit, 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."[480]

At the 2019 Osaka Summit, the G20 leaders presented the Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism, which tackled cyber security.[481] 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].

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." 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." Along with the Common Framework for Measuring the Digital Economy, the G20 ministers responsible for the digital economy presented three sets of best

[478] G20 Leaders' Communique Hangzhou Summit, RANEPA (Moscow) 05 September 2016. Access Date: 11 January 2022. https://www.ranepa.ru/images/media/g20/2016Hangzhou/G20%20Leaders%E2%80%99%20Communique%20Hangzhou%20Summit.pdf
[479] G20 Initiative "#eSkills4Girls," RANEPA (Moscow) 8 July 2017. Access Date: 11 January 2022. https://www.ranepa.ru/images/media/g20/2017hamburg/2017-g20-initiative-eskills4girls-en.pdf
[480] G20 Leaders' declaration, RANEPA (Moscow) 01 December 2018. Access Date: 11 January 2022. https://www.ranepa.ru/images/media/g20/2018buenosaires/buenos_aires_leaders_declaration.pdf
[481] 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: 11 January 2022. https://www.ranepa.ru/images/News_ciir/Project/G20_new_downloadings/G20_OSAKA_LEADERS_STATEMENT_ON_PREVENTING_EXPLOITATION_OF_THE_INTERNET_FOR_TERRORISM.pdf

practices related to ensuring Security in the Digital Economy, advancing the G20 common Principles on the AI and promoting Smart Mobility.

At the 2020 Riyadh Summit, the leaders' recognized the key role of "connectivity, digital technologies, and policies" in "strengthening our response to the pandemic and facilitating the continuation of economic activity." 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."[482]

At the 2021 Rome Summit, the ministers agreed on necessity to "embrace opportunities and address challenges and risks to further leverage the potential of digitalisation for a resilient, strong, sustainable and inclusive recovery, while tackling inequalities."[483] Regarding issues related to consumers protection in the global digital economy, the ministers committed to "take action to raise awareness, educate and support consumers, including through digital literacy programs in the digital economy, with the aim of preventing the detriment of consumers and ensuring consumer's protection regarding products' quality and safety, privacy and personal data protection, and unfair commercial practices, with particular consideration for vulnerable consumers." Commitment to "coherent and responsible data governance" along with "enforcement of intellectual property rights, taking into account differences in national legal systems"[484] were also mentioned in the Declaration's text.

The decisions agreed by the responsible ministers were approved by the G20 leaders in Rome. The leaders reaffirmed the role of data for development and agreed on continuing working on "addressing challenges such as those related to privacy, data protection, security and intellectual property rights, in accordance with the relevant applicable legal frameworks."[485]

Commitment Features

This commitment requires the G20 members to take actions aimed at promoting privacy and improving data protection; ensuring security; and enforcing intellectual property rights in accordance with the relevant applicable legal protection. To achieve full compliance, a G20 member should take action on all three key areas.

Promoting 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,[486] these aspects should not be treated separately.

"Data protection" embraces two closely intertwined but not overlapping notions of "consumer data" and "personal data." The term "consumer data" refers to data concerning consumers, where such data have been

[482] Leaders' Declaration G20 Riyadh Summit, RANEPA (Moscow) 22 November 2020. Access Date: 11 January 2022. https://www.ranepa.ru/ciir/sfery-issledovanij/gruppa-dvadtsati/dokumenty-gruppy-dvadtsati/saudovskoe-predsedatelstvo-2020/G20%20Riyadh%20Summit%20Leaders%20Declaration_EN.pdf

[483] Declaration of G20 Digital Ministers, RANEPA (Moscow) 05 August 2021. Access Date: 13 December 2021. https://www.ranepa.ru/ciir/sfery-issledovanij/gruppa-dvadtsati/dokumenty-gruppy-dvadtsati/italyanskoe-predsedatelstvo-2021/DECLARATION-OF-G20-DIGITAL-MINISTERS-2021_FINAL.pdf

[484] G20 Leaders' Declaration, RANEPA (Moscow) 31 October 2021. Access Date: 13 December 2021. https://www.ranepa.ru/ciir/sfery-issledovanij/gruppa-dvadtsati/dokumenty-gruppy-dvadtsati/italyanskoe-predsedatelstvo-2021/G20-ROME-LEADERS-DECLARATION.pdf

[485] G20 Leaders' Declaration, RANEPA (Moscow) 31 October 2021. Access Date: 13 December 2021. https://www.ranepa.ru/ciir/sfery-issledovanij/gruppa-dvadtsati/dokumenty-gruppy-dvadtsati/italyanskoe-predsedatelstvo-2021/G20-ROME-LEADERS-DECLARATION.pdf

[486] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (Paris) 2013. Access Date: 13 December 2021. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

collected, traded or used as part of a commercial relationship.[487] "Personal data" refers to "any information relating to an identified or identifiable individual (data subject).[488]

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 coordinated 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
- Ensure that there is no unfair discrimination against data subjects.[489]

Ensuring security

"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."[490] Addressing security risks is essential for economic and social prosperity. Regarding "digital security risks" the OECD notes the following:

"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."[491]

[487] Consumer Data Rights and Competition – Background note, OECD (Paris) 2013. Access Date: 13 December 2021. https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf

[488] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (Paris) 2013. Access Date: 13 December 2021. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[489] The OECD Privacy Framework, OECD (Paris) 2013. Access Date: 13 December 2021. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[490] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: 13 December 2021. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf

[491] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: 13 December 2021. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf

Ensuring 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."[492]

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 coordination 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; cooperate, 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 coordination 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;
- 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.[493]

Enforcing intellectual property rights

"Intellectual property rights" (IPR) refers to "the legal rights which result from intellectual activity in the industrial, scientific, literary and artistic fields." WIPO also specifies that these laws "aims at safeguarding

[492] 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

[493] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: 13 December 2021. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf

creators and other producers of intellectual goods and services by granting them certain time-limited rights to control the use made of those productions."[494]

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.[495]

To achieve full compliance (+1), a G20 member must 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) is awarded 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. Partial compliance will also 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. A score of non-compliance (−1) will be given to a G20 member that fails to take action towards any of the three spheres.

Scoring Guidelines

−1	G20 member does no action addressing challenges such as those related to privacy and data protection; security; and intellectual property rights, in accordance with the relevant applicable legal frameworks
0	G20 member takes actions in ONE or TWO of the areas: privacy and data protection; security; and intellectual property rights, in accordance with the relevant applicable legal frameworks
+1	G20 member takes actions in all THREE of the areas: privacy and data protection; security; and intellectual property rights, in accordance with the relevant applicable legal frameworks

Compliance director and lead analyst: Alexander Ignatov

Argentina: 0

Argentina has partially complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 30 December 2021, the Central Bank Board decided that financial institutions should hold 100 per cent of the funds deposited by payment service providers offering payment accounts in reserve to protect deposits from any unforeseen circumstances. This measure promotes "transactional nature of payment accounts while favoring the expansion of digital means of payment, and endowing them with enhanced transparency and security."[496]

[494] WIPO Intellectual Property Handbook, WIPO (Geneva) 2004. Access Date: 13 December 2021. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_489.pdf

[495] WIPO Intellectual Property Handbook, WIPO (Geneva) 2004. Access Date: 13 December 2021. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_489.pdf

[496] Electronic Wallet Funds to be Immobilized at the BCRA, BCRA (Buenos Aires) 30 December 2021. Translation provided by the analyst. Access Date: 3 March 2022. http://www.bcra.gob.ar/Noticias/fondos-billeteras-virtuales-permaneceran-encajados-en-bcra-i.asp

On 8 January 2022, following the signing of Administrative Decision 5/2022[497], Chief of the Cabinet and Minister of the Interior signed a contract with the national telecommunications company for the installation, commissioning and distribution of digital communications to provide free internet access to localities in all regions of the country. The national government is investing more than ARS289 million to reduce the digital divide across the country and achieve digital sovereignty.[498]

On 22 January 2022, the Central Bank Board presented the new standardized quick response code payment system, based on a digital, open and universal payments ecosystem. This system makes access to digital payments much easier and safer, and increases competition between service providers.[499]

On 11 February 2022, Minister of Community Innovation Daniel Filmus formally announced that the United Nations Children's Fund has joined the Gender Technology Centre. The main goal is to encourage cooperation, collaboration and exchange that will promote spread of STEM – Science, Technology, Engineering, Mathematics – skills and competencies.[500]

On 24 February 2022, the Central Bank Board established new technical requirements for payment service providers "in order to reinforce measures that mitigate fraud in transactions made through digital wallets." It improves the traceability of suspicious fraudulent transactions and maintains confidentiality.[501]

On 9 March 2022, the Financial Intelligence Unit has announced Cybersecurity Awareness Programme to provide general knowledge to protect the agency's information assets from internal and external risks.[502]

On 15 March 2022, the Ministry of Productive Development Daniel Scioli has launched a new call for the "Knowledge Economy Nodes Programme," with resources of ARS1 billion to promote investment in clusters, poles and technology parks in all provinces of the country.[503]

On 19 March 2022, Head of Cabinet Minister Juan Manzur announced the "Digital Infrastructure Development Programme" to improve digital infrastructure across the country. It foresees a loan of ARS170 million and aims to foster innovation in the digital services provided by the state through ARSAT.[504]

[497] Administrative Decision 5 / 2022, Cabinet of Ministers, (Buenos Aires) 8 January 2022. Translation provided by the analyst. Access Date: 6 March 2022. https://www.argentina.gob.ar/normativa/nacional/decisión_administrativa-5-2022-359331

[498] The national government is investing more than 289 million pesos to reduce the digital divide throughout the country, Head of Cabinet of Ministers (Buenos Aires) 8 January 2022. Translation provided by the analyst. Access Date: 5 March 2022. https://www.argentina.gob.ar/noticias/el-gobierno-nacional-invierte-mas-de-289-millones-de-pesos-para-reducir-la-brecha-digital

[499] 3.0 Transfers: more than two million transactions in interoperable environments in less than two months, BCRA (Buenos Aires) 22 January 2022. Translation provided by the analyst. Access Date: 3 March 2022. http://www.bcra.gob.ar/Noticias/Transferencias-3-0-millones-de-transacciones-realizadas-i.asp

[500] G+T Centre brings UNICEF to the public-private working table, Head of Cabinet of Ministers (Buenos Aires) 11 February 2022. Translation provided by the analyst. Access Date: 3 March 2022. https://www.argentina.gob.ar/noticias/el-centro-gt-incorpora-unicef-la-mesa-de-trabajo-publico-privada

[501] The BCRA Reinforced Measures to Improve Security of Digital Wallets, BCRA (Buenos Aires) 24 February 2022. Translation provided by the analyst. Access Date: 3 March 2022. http://www.bcra.gob.ar/Noticias/Medidas-para-evitar-fraudes-billeteras-electronicas-i.asp

[502] Cybersecurity Awareness Programme, Financial Intelligence Unit (Buenos Aires) 9 March 2022. Translation provided by the analyst. Access Date: 01 April 2022. https://www.argentina.gob.ar/noticias/programa-de-concientizacion-en-ciberseguridad

[503] Knowledge Economy Nodes in all provinces, Ministry of Productive Development (Buenos Aires) 15 March 2022. Translation provided by the analyst. Access Date: 17 June 2022. https://www.argentina.gob.ar/noticias/desarrollo-productivo-destina-1000m-para-potenciar-nodos-de-la-economia-del-conocimiento-en

[504] A programme to improve digital infrastructure across the country is moving forward with a World Bank loan, Head of Cabinet of Ministers (Buenos Aires) 19 March 2022. Translation provided by the analyst. Access Date: 17 June 2022. https://www.argentina.gob.ar/noticias/avanza-un-programa-para-mejorar-la-infraestructura-digital-en-todo-el-pais-partir-de-un

On 22 March 2022, the National Secretariat for Small and Medium-sized Enterprise has launched the Digital Transformation Programme for small and medium size enterprises (SMEs) to promote the digitalization of SMEs throughout the country by training and technical assistance.[505]

On 28 March 2022, within the framework of the Programme for Strengthening Cybersecurity and Cybercrime Investigation, the Minister of Security of the Nation signed a series of agreements to receive specific information to detect, prevent, mitigate or neutralise threats and cybercrime such as scams, cyberattacks and grooming, among other crimes.[506]

On 31 March 2022, the National Agency for the Promotion of Research, Technological Development and Innovation presented the "Federal Network of Innovative SMEs." This initiative seeks to create a space for those companies that make investment in science and technology a key element of their development to establish links, agree on work agendas and strengthen themselves through the exchange of experiences.[507]

On 8 April 2022, President Alberto Fernandez has launched the federal programmes "Construir and Equipar Ciencia," which will have an investment of ARS13 billion to acquire strategic equipment and adapt infrastructure with the aim of strengthening capacities and developing strategic opportunities in regional economies throughout the country. It will create a federal network of science and technology infrastructure to transform the production model and reduce asymmetries between provinces and regions of the country.[508]

On 11 April 2022, Minister Scioli announced the new call for Strategic Scientific and Technological Projects, which would receive funding of ARS150 million for the development of scientific and technological products, the creation of prototypes and the scaling up of production, through the Supplier Development Programme.[509]

On 11 April 2022, Minister of Economy Martín Guzmán announced to invest more than USD500,000 to the construction of the nanotechnology production area. This financing will allow to promote exports; to trade with regional and non-traditional markets such as Iran, Holland, Saudi Arabia; and to double the company's workforce.[510]

On 12 April 2022, the Secretariat of Technological Innovation of the Public Sector of the Office of the Chief of Cabinet of Ministers, through the Undersecretariat of Administrative Innovation, created the "Federal Programme of Digital Public Transformation." This initiative aims to implement digital tools for the integration

[505] Digital Transformation Workshop for SMEs, Ministry of Productive Development (Buenos Aires) 22 March 2022. Translation provided by the analyst. Access Date: 5 April 2022. https://www.argentina.gob.ar/noticias/comenzaron-las-actividades-de-las-utd-con-el-primer-taller-de-transformacion-digital-para

[506] Agreements with multinational technology companies to protect cyberspace and combat cybercrime, Ministry of Security (Buenos Aires) 29 March 2022. Translation provided by the analyst. Access Date: 5 April 2022. https://www.argentina.gob.ar/noticias/acuerdos-con-multinacionales-de-tecnologia-para-proteger-el-ciberespacio-y-combatir-los

[507] Launch of the Federal Network of Innovative SMEs, Ministry of Science, Technology and Innovation (Buenos Aires) 31 March 2022. Translation provided by the analyst. Access Date: 17 June 2022. https://www.argentina.gob.ar/noticias/se-lanzo-la-red-federal-de-pymes-innovadoras

[508] The president announced a $13 billion investment in federal science and technology development, Casa Rosada Presidencia (Buenos Aires) 8 April 2022. Translation provided by the analyst. Access Date: 17 June 2022. https://www.casarosada.gob.ar/slider-principal/48658-el-presidente-anuncio-una-inversion-de-13-mil-millones-para-el-desarrollo-federal-de-la-ciencia-y-la-tecnologia

[509] New call for proposals to fund projects to boost the national scientific and technological industry, Ministry of Productive Development (Buenos Aires) 11 April 2022. Translation provided by the analyst. Access Date: 17 June 2022. https://www.argentina.gob.ar/noticias/nueva-convocatoria-para-financiar-proyectos-que-impulsen-la-industria-cientifico

[510] Medical supply SME announces USD 500,000 investment in nanotechnology development, Ministry of Economy (Buenos Aires) 11 April 2022. Translation provided by the analyst. Access Date: 17 June 2022. https://www.argentina.gob.ar/noticias/pyme-de-insumos-medicos-le-anuncio-guzman-inversiones-por-usd-500000-para-el-desarrollo-de

of systems for the simplification of procedures and digital signature throughout the public sector; streamline administrative processes and generate digital documents.[511]

On 14 May 2022, Secretary of Industry, Knowledge Economy and External Trade Management Ariel Schale presented the second edition of "Soluciona" programme, with an initial budget of ARS25 million to finance projects of companies, universities and cooperatives that incorporate or develop Knowledge Economy for their products and services.[512]

On 10 June 2022, in the framework of "Empowering Communities," one of the pillars of the initiative promoted by the International Telecommunication Union, Sanchez Malcolm stressed that Argentina aims to reach 70 per cent digitised jurisdictions by 2026, which implies an investment of at least ARS12 million. The goal of the federal Digital Public Transformation programme is to transfer resources to digitize the country's 24 provincial and 2,300 local governments.[513]

Argentina has taken steps to address challenges such as those related to privacy and data protection, and security. However, no action aimed to tackle challenges related to intellectual property rights has been found during the monitoring period.

Thus, Argentina receives a score of 0.

Analyst: Elena Alekseeva

Australia: 0

Australia has partially complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 6 December 2021, the government released an update to the Digital Government Strategy. The update is set as to promote the government's digital capabilities, including provision of reliable access to public data.[514]

On 25 May 2022, Australia joined the Quad Partnership on Critical technology Supply Chains together with Japan, the United States and India. The parties agreed to set a joint cyber security principles to provide better cybersecurity of critical infrastructure.[515]

Australia has taken steps to address challenges such as those related to privacy and data protection, and security. However, no action aimed to tackle challenges related to intellectual property rights has been found during the monitoring period.

[511] The Secretariat for Technological Innovation created the Federal Programme for Digital Public Transformation. Head of Cabinet of Ministers (Buenos Aires) 12 April 2022. Translation provided by the analyst. Access Date: 17 June 2022. https://www.argentina.gob.ar/noticias/la-secretaria-de-innovacion-tecnologica-creo-el-programa-federal-de-transformacion-publica

[512] Knowledge economy projects, Ministry of Productive Development (Buenos Aires) 14 May 2022. Translation provided by DeepL Translate. Access Date: 17 June 2022. https://www.argentina.gob.ar/noticias/desarrollo-productivo-financiara-proyectos-de-la-economia-del-conocimiento-por-hasta-25

[513] Argentina participated in the first annual meeting of the Partner2Connect Digital Coalition. Head of Cabinet of Ministers (Buenos Aires) 10 June 2022. Translated by DeepL Translate. Access Date: 17 June 2022. https://www.argentina.gob.ar/noticias/argentina-participo-de-la-primera-reunion-anual-de-partner2connect-digital-coalition

[514] Digital Government Strategy to make Australia a world leading digital government, Ministers' Media Centre (Canberra) 6 December 2021. Access Date: 10 June 2022. https://ministers.dese.gov.au/robert/digital-government-strategy-make-australia-world-leading-digital-government

[515] Quad Cybersecurity Partnership Joint Principles and Common Statement of Principles on Critical Technology Supply Chains, CISC News (Canberra) 25 May 2022. Access Date: 10 June 2022. https://www.cisc.gov.au/news-media/archive/article?itemId=900

Thus, Australia receives a score of 0.

Analyst: Alexander Ignatov

Brazil: +1

Brazil has fully complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 7 December 2021, Brazil adopted the Decree No. 10,886 on National Intellectual Property Strategy. It is established for the period from 2021 to 2030 with the objective of defining long-term actions for the coordinated action to establish an effective and balanced National System of Intellectual Property.[516]

On 10 February 2022, Constitutional Amendment (EC) 115/2022 was enacted. It includes the protection of personal data among fundamental rights and guarantees. It also establishes the Union's private competence to legislate on the protection and processing of personal data, in accordance with the General Data Protection Law.[517]

On 14 March 2022, President Jair Bolsonaro signed the Decree No. 10996, which amends the 2020-2022 Digital Government Strategy for the Federal Public Administration. The change aims to further improve the quality of services gathered on the GOV.BR platform. The new text also highlights the importance of unifying digital channels in GOV.BR, the interoperability of government systems (data integration), and security and privacy, in line with the General Law for the Protection of Personal Data.[518]

On 18 March 2022, it was announced that public services with relevant access offered on the digital platform for the relationship between citizens and the Brazilian government, GOV.BR, will begin to require higher levels of security for validation. This update of security requirements occurs with services that involve access to sensitive information or the payment of benefits by the government, such as, for example, some of the National Institute of Social Security. A practical action to increase the level of security in GOV.BR accounts is bank validation.[519]

On 20 June 2022, the Ministry of Economy published operational guide with guidelines to expand the protection of critical government systems and encourage the use of safer practices in the bodies and entities of the Federal Public Administration. The Vulnerability Management Guide focuses on building routine processes for managing vulnerability cycles in the organization's data protection and security. The measure is part of the Privacy and Information Security Program to increase the level of maturity of the bodies in terms of protection of personal data and information security actions.[520]

[516] Decree No. 10,886, of December 7, 2021, Diário Oficial Da União (Brasilia) 7 December 2021. Translation provided by the analyst. Access Date: 4 April 2022. https://www.in.gov.br/web/dou/-/decreto-n-10.886-de-7-de-dezembro-de-2021-365433440.
[517] Protection of personal data is included among the fundamental rights of the citizen, Brazilian Government (Brasilia) 10 February 2022. Translation provided by the analyst. Access Date: 4 April 2022. https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/fevereiro/protecao-de-dados-pessoais-e-incluida-entre-direitos-fundamentais-do-cidadao.
[518] Published decree that improves Digital Government Strategy for the period from 2020 to 2022 and includes GovTechs, Brazilian Government (Brasilia) 14 March 2022. Translation provided by the analyst. Access Date: 4 April 2022. https://www.gov.br/governodigital/pt-br/noticias/publicado-decreto-que-aprimora-estrategia-de-governo-digital-para-o-periodo-de-2020-a-2022-e-inclui-govtechs.
[519] Bank validation aims to increase the security level of GOV.BR accounts, Brazilian Government (Brasilia) 14 March 2022. Translation provided by the analyst. Access Date: 4 April 2022. https://www.gov.br/governodigital/pt-br/noticias/validacao-bancaria-visa-aumentar-o-nivel-de-seguranca-das-contas-no-gov.br
[520] Economy launches guidance on privacy and information security aimed at public bodies, Brazilian Government (Brasilia) 20 June 2022. Translation provided by the analyst. Access Date: 20 June 2022. https://www.gov.br/economia/pt-br/assuntos/noticias/2022/junho/economia-lanca-guia-de-orientacao-sobre-privacidade-e-seguranca-da-informacao-voltados-a-orgaos-publicos.

Brazil took actions in all three areas of the commitment: privacy and data protection; security; and intellectual property rights.

Thus, Brazil receives a score of +1.

Analyst: Irina Popova

Canada: +1

Canada has fully complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 9 December 2021, the final annual report of the Privacy Commissioner's mandate was presented in Parliament of Canada. The report focuses on the growing challenges for privacy and steps that should be made to provide security of personal data. Daniel Therrien, the Commissioner, insists that the government ought to act as recommended in a recent declaration of G7 Digital and Technology Ministers. It calls for implementation of a "sustainable, inclusive and human-centric" approach to a post-pandemic prosperity that is guided by common democratic values of open competitive markets. The main idea of the report is to limit governmental activities aimed at collecting personal information of citizens within the framework of the Privacy Act.[521]

On 1 February 2022, the Intellectual Property Office started the process of becoming a depositing office for patent applications for the World Intellectual Property Organization (WIPO) Digital Access Service (DAS). The DAS is a digital library service administered by WIPO that facilitates the secure exchange of priority documents between intellectual property offices. This initiative will simplify the patent application process for clients who have a priority claim in Canada. By making a copy of their application easily available on DAS, applicants will save time and effort on their international filings at participating offices.[522]

On 10 March 2022, the Office of the Privacy Commissioner of Canada (OPC) has renewed and updated a Memorandum of Understanding (MOU) with Autoriteit Persoonsgegevens, the data protection authority for the Netherlands, to facilitate information sharing between the two organizations. The OPC has signed similar memorandums of understanding with a number of other data protection authorities as part of the goal of protecting personal information. The Office is committed to collaborating with partners in Canada and internationally. The updated MOU will replace an earlier version of the agreement which was first signed in 2011.[523]

On 2 May 2022, the heads of Canada's privacy protection authorities issued a joint statement recommending legislators develop a legal framework that establishes clearly and explicitly the circumstances in which police use of facial recognition may be acceptable.[524]

On 6 June 2022, the OPC announced that it signed a Memorandum of Understanding with the Commissioner of Data Protection of the Abu Dhabi Global Market to facilitate information sharing between the two organizations. The OPC has signed similar memorandums of understanding with a number of other data

[521] To build a more resilient economy, Commissioner calls on government to make privacy law reform a priority, Office of the Privacy Commissioner (Gatineau) 9 December 2021. Access Date: 20 February 2022 https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_211209/

[522] CIPO to become a Digital Access Service depositing office for patent applications, Government of Canada (Ottawa) 1 February 2022. Access Date: 20 February 2022 https://www.canada.ca/en/intellectual-property-office/news/2022/02/cipo-to-become-a-digital-access-service-depositing-office-for-patent-applications.html

[523] OPC updates its information-sharing agreement with the Dutch data protection authority, Office of the Privacy Commissioner of Canada, 10 March 2022. Access Date: 18 June 2022 https://priv.gc.ca/en/opc-news/news-and-announcements/2022/an_220310/

[524] Privacy regulators call for legal framework limiting police use of facial recognition technology, Office of the Privacy Commissioner of Canada, 2 May 2022. Access Date: 18 June 2022 https://priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220502/

protection authorities as part of the goal of protecting personal information. The OPC is committed to collaborating with partners in Canada and internationally.[525]

On 15 June 2022, François-Philippe Champagne, Minister of Innovation, Science and Industry, and David Lametti, Minister of Justice and Attorney General of Canada, held a media statement on proposed legislation that includes a new privacy regime to increase transparency and give Canadians more control over their data and new rules to help ensure the responsible use of AI, building trust in the digital economy.[526]

On 16 June 2022, Minister Champagne together with Minister of Justice and Attorney General David Lametti, introduced the Digital Charter Implementation Act, 2022, which is said to significantly strengthen Canada's private sector privacy law, create new rules for the responsible development and use of artificial intelligence, and continue advancing the implementation of Canada's Digital Charter. As such, the Digital Charter Implementation Act, 2022 includes three proposed acts: the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act. The proposed Consumer Privacy Protection Act will address the needs of Canadians who rely on digital technology and respond to feedback received on previous proposed legislation. This law will ensure that the privacy of Canadians will be protected and that innovative businesses can benefit from clear rules as technology continues to evolve. The proposed Personal Information and Data Protection Tribunal Act will enable the creation of a new tribunal to facilitate the enforcement of the Consumer Privacy Protection Act.[527]

Canada has taken actions in all three key areas of the commitment – privacy and data protection; security and intellectual property rights.

Thus, Canada receives a score of +1.

Analyst: Nikita Shilikov

China: +1

China has fully complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 1 November 2021, the law on protecting online user data privacy came into force in China. The law states that handling of personal information shall be limited to the minimum scope necessary to achieve the goals of handling data. Moreover, it lays out conditions for which companies can collect personal data, including obtaining an individual's consent, as provides guidelines for ensuring data protection when data is transferred outside the country.[528]

On 1 November 2021, China and Russia held a meeting on cooperation in information and communication sphere. The parties discussed issues related to network security, mailing and broadband spectrum usage in

[525] OPC signs information-sharing agreement with the data protection authority of Abu Dhabi, Office of the Privacy Commissioner of Canada, 6 June 2022. Access Date: 18 June 2022 https://priv.gc.ca/en/opc-news/news-and-announcements/2022/an_220603/
[526] Government of Canada to hold technical briefing and media availability on strengthening Canadians' protection and trust in the digital economy, Government of Canada (Ottawa) 15 June 2022. Access Date: 18 June 2022 https://www.canada.ca/en/innovation-science-economic-development/news/2022/06/government-of-canada-to-hold-technical-briefing-and-media-availability-on-strengthening-canadians-protection-and-trust-in-the-digital-economy.html
[527] New laws to strengthen Canadians' privacy protection and trust in the digital economy, Government of Canada (Ottawa) 16 June 2022. Access Date: 18 June 2022 https://www.canada.ca/en/innovation-science-economic-development/news/2022/06/new-laws-to-strengthen-canadians-privacy-protection-and-trust-in-the-digital-economy.html
[528] China passes new personal data privacy law, to take effect Nov. 1, Reuters (Beijing) 20 August 2021. Access Date: 1 April 2022. https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/.

neighboring regions of the two countries. The counterparts agreed on initiation of several bilateral projects in the respective sphere.[529]

On 9 November 2021, the Foreign Ministry announced it would further promote the opening up of intellectual property rights at a deeper level, as well as strengthen international cooperation with all parties, including the World Intellectual Property Organization (WIPO), in order to make contribution "to the balanced, inclusive and sustainable development of global IPRs" in line with the new 5-year plan for IPRs.[530]

On 21 January 2022, China Banking and Insurance Regulatory Commission announced measures for the regulation of information technology outsourcing activities in banking and insurance institutions to further strengthen risk management. The new regulations required banking and insurance institutions to reduce their reliance on a few information technology (IT) providers outsourcing service providers, conduct onsite inspections of offsite outsourcing services which meet the standards for important IT outsourcing activities, carry out comprehensive IT outsourcing risk management evaluation at least once a year, as well as conduct audit work on this type of outsourcing activities regularly.[531]

China has taken actions in all three of the areas: privacy and data protection; security; and intellectual property rights, in accordance with the relevant applicable legal frameworks.

Thus, China receives a score of +1.

Analyst: Andrey Shelepov

France: 0

France has partially complied with the commitment address challenges related to privacy, data protection, security and intellectual property rights.

On November 2, 2021, Secretary of State for Digital Transition and Electronic Communications Cédric O, presented the industrial plan to support the French Cloud sector, the last pillar of the national Cloud strategy announced in May 2021 jointly by Minister of the Economy and Finance Bruno Le Maire and Minister of Public Transformation and Service Amélie de Montchalin. Symbolically, Secretary O presented this strategy to OVHcloud, the first European player to climb into the world's top 10 cloud providers. This economic plan constitutes the third pillar of the national strategy for the Cloud Industry, following the new doctrine "Cloud at the center" to transform public authorities and the promotion of trusted offers from the SecNumCloud. This component, endowed with EUR1.8 billion, including EUR667 million in public funding, EUR680 million in private co-financing and EUR444 million in European funding, is part of the 4th Investments for the Future Program and France Relance. This strategy relies on innovation and the strengths of French cloud providers by:

- supporting the development of innovative French offers, including free software;
- accelerating the scaling up of French players on critical technologies in high demand, such as big data or collaborative work;
- ensuring data protection;

[529] Russia and China to discuss ICT development, Ministry of Digital Development, Connection and Mass Communication of the Russian Federation (Moscow) 1 November 2021. Translation provided by the analyst. Access Date: 01 March 2022. https://digital.gov.ru/ru/events/41348/

[530] China to further expand international IPR cooperation: Foreign Ministry, Global Tims (Beijing) 9 November 2021. Access Date: 1 April 2022. https://www.globaltimes.cn/page/202111/1238517.shtml.

[531] Regulator issues measures on IT outsourcing to strengthen risk management, China Daily (Beijing) 21 January 2022. Access Date: 1 April 2022. https://global.chinadaily.com.cn/a/202201/21/WS61ea7761a310cdd39bc8287a.html.

- intensifying the development of breakthrough technologies by 2025, such as edge computing in order to position the European sector as a future champion.

This strategy is the result of the public consultations carried out with the players in the sector, in particular within the framework of the CSF security industry, major European projects and partnerships and the call for expressions of interest launched at the beginning of the year.[532]

France has taken steps to tackle issues related to digital users' data privacy protection. However, no action aimed at providing digital security and dealing with intellectual property rights issues has been found within the monitoring period.

Thus, France receives a score of 0.

Analyst: Nikita Shilikov

Germany: +1

Germany has fully complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights (IPRs).

On 11 November 2021, the European Parliament adopted a resolution on an intellectual property action plan aimed at supporting the EU's recovery and resilience. It notes the importance of balanced protection and enforcement of IPRs to the European economy as well as to the EU's recovery and resilience, in particular to the COVID-19 pandemic. The plan follows the Commission's IP Action Plan adopted in November 2020 and addresses a number of strategies for the protection and enforcement of IPRs.[533]

On 14 December 2021, the European Data Protection Board (EDPB) adopted the Guidelines on Examples regarding Personal Data Breach Notification. The Guidelines provide practice-oriented, case-based guidance, that utilizes the experiences gained by supervisory authorities since the General Data Protection Regulation is applicable.[534]

On 28 January 2022, the EDPB published new guidelines on individuals' right to access their data, including that held by employers and former or prospective employers.[535]

On 15 March 2022, the EU, the US, India and South Africa reached agreement on a proposed patent waiver for COVID-19 vaccines related to the Agreement on Trade-Related Aspects of Intellectual Property. The proposal would permit an "eligible" World Trade Organization (WTO) member to temporarily authorize use of patented inventions necessary for COVID-19 vaccine production and supply, without the right holder's consent. An eligible member would be any developing country member that exported less than 10 per cent of world exports of COVID-19 vaccines in 2021. It could use any instrument available in law to make the authorization.[536]

[532] Investments for the future | Cédric O announces an innovation strategy of nearly €1.8 billion to support the French Cloud industry, Government of France (Paris) 2 November 2021. Translation provided by Google Translate. Access Date: 20 February 2022. https://www.gouvernement.fr/investissements-d-avenir-cedric-o-annonce-une-strategie-d-innovation-de-pres-de-18mdseu-pour
[533] An intellectual property action plan to support the EU's recovery and resilience, European Parliament (Brussels) 11 November 2021. Access Date: 20 June 2022. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0453_EN.pdf.
[534] Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, European Data Protection Board (Brussels) 3 January 2022. Access Date: 1 April 2022. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en.
[535] Guidelines 01/2022 on data subject rights - Right of access, European Data Protection Board (Brussels) 28 January 2022. Access Date: 1 April 2022. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en.
[536] Breakthrough on a Potential COVID-19 Intellectual Property Rights Waiver, Congressional Research Service (Washington) 25 March 2022. Access Date: 20 June 2022. https://crsreports.congress.gov/product/pdf/IN/IN11901.

Germany has taken actions in all three of the areas: privacy and data protection; security; and intellectual property rights, in accordance with the relevant applicable legal frameworks.

Thus, Germany receives a score of +1.

Analyst: Andrey Shelepov

India: +1

India has fully with the commitment to address challenges related to privacy, data protection, security and intellectual property rights (IPRs).

On 18 November 2021, Union Minister for Electronics and Information Technologies (IT), Communications and Railways Ashwini Vaishnaw and Union Minister of State for Electronics and IT, Skill Development and Entrepreneurship Rajeev Chandrasekhar announced the winners of the Cyber Security Grand Challenge. The Challenge is aimed at promoting innovation and entrepreneurship in the country. The winners of Grand Challenge were awarded with a trophy each and cash prize money of INR10 million to the winner, INR6 million to the first runner-up and INR4 million to the second runner-up.[537]

On 16 December 2021, the Joint Parliamentary Committee (JPC) presented its report on the Personal Data Protection (PDP) Bill 2019 in both Houses of Indian Parliament. The committee highlighted that the PDP Bill should cover both personal and non-personal data till an additional framework is established to distinguish between them. The JPC also suggested that no social media platform be permitted to operate in India unless the parent company in charge of the technology sets up an office in the country.[538]

On 10 March 2022, Union Minister for micro, small and medium-sized enterprises (MSMEs) Narayan Rane launched the MSME Innovative Scheme (Incubation, Design and IPR). MSME Innovative Scheme is a tool to unify, synergize and converge three sub-components and interventions with a single purpose. In terms of IPRs the objective of the scheme is to improve the IP culture in India with a view to enhance the awareness among MSMEs. It also aims to take measures for the protection of ideas, technological innovation and knowledge-driven business strategies developed by the MSMEs for their commercialization and effective utilization of IPR tools through IP Facilitation Centre and relevant financial assistance.[539]

On 15 March 2022, the EU, the US, India and South Africa reached agreement on a proposed patent waiver for COVID-19 vaccines related to the Agreement on Trade-Related Aspects of Intellectual Property. The proposal would permit an "eligible" World Trade Organization member to temporarily authorize use of patented inventions necessary for COVID-19 vaccine production and supply, without the right holder's consent. An eligible member would be any developing country member that exported less than 10 per cent of world exports of COVID-19 vaccines in 2021. It could use any instrument available in law to make the authorization.[540]

India has taken actions in all three of the areas: privacy and data protection; security; and intellectual property rights, in accordance with the relevant applicable legal frameworks.

[537] Ministry of Electronics & IT and DSCI felicitated Start-ups under the 'Cyber Security Grand Challenge' with a total prize money of INR 3.2 Cr, Data Security Council of India (New Delhi) 18 November 2021. Access Date: 1 April 2022. https://www.dsci.in/sites/default/files/Press%20Release-Cyber%20Security%20Grand%20Challenge.pdf.
[538] What The JPC Report On The Data Protection Bill Gets Right And Wrong, The Wire (New Delhi) 20 December 2021. Access Date: 1 April 2022. https://thewire.in/tech/what-the-jpc-report-on-the-data-protection-bill-gets-right-and-wrong
[539] Shri Narayan Rane launches MSME Innovative Scheme (Incubation, Design and IPR) & MSME IDEA HACKATHON 2022 under MSME Champions Scheme, Indian Prime Minister's Office (New Delhi) 10 March 2022. Access Date: 1 April 2022. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1804723.
[540] Breakthrough on a Potential COVID-19 Intellectual Property Rights Waiver, Congressional Research Service (Washington) 25 March 2022. Access Date: 20 June 2022. https://crsreports.congress.gov/product/pdf/IN/IN11901.

Thus, India receives a score of +1.

Analyst: Andrey Shelepov

Indonesia: 0

Indonesia has partially complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 20 December 2021, The Directorate General of Intellectual Property of the Ministry of Law and Human Rights of the Republic of Indonesia (DGIP) issued the decision on Implementation of Automatic Approval in Copyright Recordation System; the purpose of the system is to provide legal certainty and increase the confidence of copyright owners through automatic acceptance and processing of requests for copyright recording and automatic approvals upon compliance with certain conditions.[541]

On 25 March 2022, the House of Representatives suspended further discussions on the Personal Data Protection and Cyber Security Bill. The government suggested that this institution should be overseen by a State Ministry, but House legislators rejected the idea claiming that the authority should be independent.[542]

On 23 May 2022, it was reported that Indonesia had plans to develop National Intellectual Property Strategy as a major step to boosting economic growth and supporting national development through the intellectual property ecosystem.[543]

On 14 June 2022, Indonesia passed the draft Law on Personal Data Protection (PDP) in response to the growing need for stronger legislative framework to protect personal data and ensure the public's right to personal data protection (though there was no indication on when it would be enacted); the draft Law covers all forms of data processing including acquisition and collection, processing and analyzing, storing, updating and correcting, displaying, announcing, transferring, disseminating, disclosing, deleting or destroying. Through the PDP Bill, the government manifests its commitment to the strengthening of personal data protection in Indonesia in the public interest.[544]

Indonesia has taken actions in data and intellectual property rights protection, in accordance with the relevant applicable legal frameworks. However, no action taken as to tackle security issues was found.

Thus, Indonesia receives the score of 0.

Analyst: Pavel Doronin

Italy: +1

Italy has fully complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 8 November 2021, the Legislative Decree No. 177 entered into effect in Italy. This legislation includes updates to copyright law in regards to the digital aspects of intellectual property rights. According to the new legislation, online service providers must recognize the exclusive reproduction and communication rights of online news publications, defined as "literary works of a reportorial nature." The Decree also contains sweeping

[541] Indonesia: The Directorate General of Intellectual Property implements the automatic recordation approval system for copyrights, Lexology – Baker McKenzie (Jakarta Office) 4 February 2022. Access Date: 31 March 2022. https://www.lexology.com/library/detail.aspx?g=26bb90b2-d277-4d5d-8c8d-bb5daadf7a25

[542] Personal Data Protection Bill Hampered by Arduous Discussions on Management, Tempo.co (Jakarta) 25 March 2022. Access Date: 31 March 2022. https://en.tempo.co/read/1574708/personal-data-protection-bill-hampered-by-arduous-discussions-on-management

[543] Indonesia to Establish National Intellectual Property Strategy, OpenGov Asia 23 May 2022. Access Date: 20 June 2022. https://opengovasia.com/indonesia-to-establish-national-intellectual-property-strategy/

[544] Indonesia's draft law on data protection to bring clarity to regulation of data handling and e-commerce, JD Supra (Jakarta) 14 June 2022. Access Date: 20 June 2022. https://www.jdsupra.com/legalnews/indonesia-s-draft-law-on-data-5705018/

changes in compensatory requirements, educational and research use of information, as well as definition and scope of requirements concerning Online Content Sharing Service Providers.[545]

On 24 May 2022, the National Cybersecurity Strategy 2022-2026 was published. The Strategy contains 82 measures on three major issue areas: protection of national strategic assets; response to national cyber threats, incidents and crises; and development of digital technologies, research, and industrial competitiveness. The Strategy, as well as the corresponding Implementation Plan, provide for a wide array of policy actions, including: development of protection capacities for national infrastructures; promotion of the use of cryptography; enhancement of public administration cyber capabilities; tackling cybercrime; supporting industrial, technological and research development. [546]

Italy took action to promote privacy and data protection; security; and intellectual property rights.

Thus, Italy is awarded a score of +1.

Analyst: Andrei Sakharov

Japan: +1

Japan has fully complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 28 September 2021, the cabinet adopted a revised Cybersecurity Strategy; the purpose of the strategy is to make cyber space "a free, fair and secure space" based on the principles of (i) assurance of the free flow of information, (ii) rule of law, (iii) openness, (iv) autonomy, and (v) collaboration among multi-stakeholders. The strategy's policy approaches cover four main areas, namely, (1) enhancing socio-economic vitality and sustainable development (through raising awareness among executives, local regions and SMEs, building a foundation for ensuring trustworthiness of supply chains that support new value creation, and advancing digital security literacy with no one left behind), (2) realizing a digital society where people can live with a sense of safety and security (through providing a cybersecurity environment that protects the people and society, ensuring cybersecurity integral with digital transformation, promotion of efforts by stakeholders which underpin the socio-economic infrastructure, ensuring seamless information sharing and collaboration among multiple stakeholders, and enhancement of readiness to respond to massive cyberattacks), (3) contributing to the peace and stability of the international community and Japan's national security (through ensuring "a free, fair and secure space," strengthening Japan's capabilities and international cooperation), and (4) cross-cutting approaches to cybersecurity (including advancement of R&D, recruitment, development and active use of human resources, and collaboration based on full participation and awareness raising).[547]

On 25-29 October 2021, the Japan–U.S. Industrial Control Systems (ICS) Cybersecurity Week was held as the fourth iteration of the Japan-U.S. ICS cybersecurity exercise, which aims to improve the security of critical cyber infrastructure in partner countries across the Indo-Pacific region; Cybersecurity Week provided participants with unique opportunities to conduct hands-on training remotely and study a variety of cybersecurity-related topics, including supply chains, process automation, and workforce development from experts from the United States, Japan, and the EU.[548]

[545] Legislative Decree 8 November 2021, n. 177, Gazzetta Ufficiale della Repubblica Italiana 8 November 2021. Access Date: 21 June 2022. https://www.gazzettaufficiale.it/eli/id/2021/11/27/21G00192/sg.
[546] National Cybersecurity Strategy 2022 – 2026, Agenzia per la Cybersicurezza Nazionale 24 May 2022. Access Date: 21 June 2022. https://www.acn.gov.it/ACN_EN_Strategia.pdf
[547] Cybersecurity Strategy, Japan's National Center of Incident Readiness and Strategy for Cybersecurity (Tokyo) 28 September 2021. Access Date: 31 March 2022. https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf
[548] Japan-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region 2021, US Mission Japan (Tokyo) 1 November 2021. Access Date: 31 March 2022. https://jp.usembassy.gov/japan-us-eu-cybersecurity-press-release/

On 30 November 2021, the government announced that it would require that website operators give internet users a way to keep their browsing data out of the hands of third parties as it moves to address growing privacy and security concerns.[549]

On 14 December 2021, the government adopted the basic policy for helping developing countries to improve their capacity in the field of cybersecurity; under the policy, Japan will expand the scope of its aid to cover economies in the Indo-Pacific region, after focusing its support in the field on member states of the Association of Southeast Asian Nations.[550]

On 20 December 2021, the government announced that it is considering to formally oblige the companies in key infrastructure sectors such as finance, telecom and transport to introduce plans for coping with cyberattacks, in response to a rise in such incidents globally.[551]

On 12 January 2022, the Patent Office announced that the gazette of published patents would be provided on a daily basis rather than a weekly basis. [552]

On 2 February 2022, the government announced that it would consider imposing tighter curbs on companies in security-sensitive sectors that procure overseas software as part of efforts to ramp up steps to counter cyberattacks; the proposal provides for crafting legislation that allows the government to order companies in such sectors as energy, water supply, information technology, finance and transportation and others critical to national security to provide advance information when updating software or procuring new equipment, and vet purchases that could put Japan at risk of cyberattacks.[553]

On 1 April 2022, an amendment to Japan's privacy and data protection law, the Act on the Protection of Personal Information ("APPI"), came into force. The APPI, applies to and regulates the privacy and data protection activities of any business that is considered a personal information handling business operator. One of the biggest shifts under the APPI amendments are the new requirements placed on businesses that transfer personal information from Japan to another location. Beginning April 2022, businesses within the scope of the APPI need to either (i) obtain an individual's opt-in consent prior to transferring that individual's personal information to a location outside of Japan; or (ii) establish a personal information protection system with the party receiving the personal in the foreign jurisdiction. The amended APPI also introduces new categories of regulated information; one of which is sensitive personal information, which is referred to as "special care-required personal information." Under the APPI, sensitive personal information includes any information about an individual's race, creed, social status, medical history, criminal records, crime victim's history, or any other information that may lead to social discrimination or disadvantage. Businesses within the scope of the APPI cannot collect or use an individual's sensitive personal information without first obtaining their prior, opt-in consent. Additionally, under the newly amended APPI, businesses within the scope of the law must report a data breach to the Personal Information Protection Commission if the breach includes: (i) sensitive information; (ii) data that could result in significant economic loss (i.e., financial information); (iii) an "unjust

[549] Japan to give internet users more control of their browsing data, Nikkei Asia (Tokyo) 30 November 2021. Access Date: 31 March 2022. https://asia.nikkei.com/Politics/Japan-to-give-internet-users-more-control-of-their-browsing-data

[550] Japan to Help Developing Nations Improve Cybersecurity, Nippon.com (Tokyo) 14 December 2021. Access Date: 31 March 2022. https://www.nippon.com/en/news/yjj2021121401049/

[551] Japan to require cyber defenses at infrastructure companies, Nikkei Asia (Tokyo) 20 December 2021. Access Date: 31 March 2022. https://asia.nikkei.com/Business/Technology/Japan-to-require-cyber-defenses-at-infrastructure-companies

[552] Japan: IP News Bulletin For Japan And China – January 2022, Mondaq – Sonoda & Kobayashi Intellectual Property Law (Tokyo), 2 February 2022. Access Date: 31 March 2022. https://www.mondaq.com/trademark/1156860/ip-news-bulletin-for-japan-and-china-january-2022

[553] Japan eyes tighter curbs on firms to counter cyberattacks, Al Jazeera 2 February 2022. Access Date: 31 March 2022. https://www.aljazeera.com/economy/2022/2/2/japan-eyes-tighter-curbs-on-firms-to-counter-cyberattacks

purpose," such as personal information hijacked by ransomware; or (iv) more than 1,000 individuals' personal information.[554]

On 4 April 2022, the Ministry of Defense announced its plans to introduce stricter cybersecurity standards for its domestic contractor companies to protect against possible cyber-attacks on the defense industry, and to prevent the leakage of sensitive national security information.[555]

Japan has taken strong actions on privacy and data protection; digital security; and intellectual property rights protection.

Thus, Japan receives a score of +1.

Analyst: Pavel Doronin

Korea: +1

Korea has fully complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 6 January 2022, the Fair Trade Commission released its proposed Guidelines for Review of Abuse of Dominance and Unfair Trade Practices by Online Platform Operators ("Proposed Guidelines") for public comment. The Proposed Guidelines are intended to make its enforcement in the online platform sector more reasonable and enhance predictability.[556]

On 12 April 2022, the Personal Information Protection Commission (PIPC) announced the standardisation initiative for the MyData programme, which is currently used for financial services and the public sector, to be introduced in all fields where general personal information is transmitted for the facilitation of transactions and disclosure. Moreover, the PIPC noted that this initiative will make different data formats and transmission methods to become unified, and that to achieve this harmonisation between fields the PIPC will introduce common standards for MyData, a glossary, specifications for procedures of different types of trasmissions, transmission standards, and a MyData certification security system.[557]

On 21 April 2022, Korea joined a multilateral agreement with Japan, the United States, Singapore, Canada, the Philippines and Chinese Taipei on cross-border data transfer privacy regulation. The agreement came out after a series of negotiations supported by the Asia-Pacific Economic Cooperation Forum. The parties therefore established the Global Cross-Border Privacy Rules Forum that is said to establish an international certification system based on the existing APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems, enabling participation beyond APEC member economies.[558]

[554] Amended Japanese Privacy Law Creates New Categories of Regulated Personal Information and Cross-Border Transfer Requirements, Lexology – Benesch Friedlander Coplan & Aronoff LLP (Cleveland) 14 March 2022. Access Date: 31 March 2022. https://www.lexology.com/library/detail.aspx?g=f66e70a4-7cdd-466a-bc1f-fe40ca5cdf66

[555] Japan's Defense Ministry to stiffen cybersecurity standards, Asia News – The Japan News (Tokyo) 4 April 2021. Access Date: 4 April 2022. https://asianews.network/japans-defense-ministry-to-stiffen-cybersecurity-standards/

[556] KFTC Issues Advance Notice of Proposed Guidelines for Review of Abuse of Dominance and Unfair Trade Practices by Online Platform Operators, Kin & Chang (Seoul) 12 January 2022. Access Date: 10 June 2022. https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=24539

[557] Personal Information Commission begins standardization of My Data in all fields, Personal Information Protection Commission (Seoul) 12 April 2022. Translation provided by Google Translate. Access Date: 10 June 2022. https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7959#LINK

[558] Global Cross-Border Privacy Rules Declaration, the U.S. Department of Commerce (Washington D.C.) 21 April 2022. Access Date: 10 June 2022. https://www.commerce.gov/global-cross-border-privacy-rules-declaration

Korea has taken strong actions on privacy and data protection; digital security; and intellectual property rights protection.

Thus, Korea receives a score of +1

Analyst: Alexander Ignatov

Mexico: +1

Mexico has fully complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 1 December 2021, the Federal Institute of Telecommunications and the National Commission for the Protection and Defense of Users of Financial Services signed a general collaboration agreement to promote trust in the digital ecosystem and foster the culture of cybersecurity. With the signing of this agreement, both institutions establish the general bases for coordination, collaboration and execution of actions, within the framework of their respective attributions and spheres of competence, to promote the responsible use of digital services and, in particular, to promote the secure Internet access and confidence in conducting financial transactions online.[559]

On 6 December 2021, the Institute of Industrial Property (IMPI) organized, in conjunction with the Universidad Panamericana, the online seminar on the Federal Law for the Protection of Industrial Property, which came into effect on November 5 of the year 2020. The purpose of the seminar was to provide an overview of intellectual property and its role as a driving force in development, to explain the general concepts on the matter, to publicize the new provisions provided for in the new Federal Law for the Protection of Industrial Property, and to promote interest in law students and lawyers in the legal framework of industrial property in Mexico for the protection of innovation and creativity.[560]

On 13 December 2021, the government issued a detailed factsheet for U.S.-Mexico High-Level Economic Dialogue in collaboration with the United States government. Cooperation on Pillar III: "Securing the Tools for Future Prosperity" includes actions in the field of cybersecurity. Parties agreed to promote opportunities to strengthen cybersecurity protections in global supply chains, facilitate collaboration and cooperation in tackling cybersecurity challenges through international industry practices and standards. Mexico and the US also plan to develop digital cooperation on cross-border privacy rules. They will "seek cooperation at the global and regional level to promote the free flow of data, as well as the interoperability of privacy and data protection rules." The United States and Mexico intend to "coordinate on a joint campaign to promote the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules system among Mexican and U.S. industries.[561]"

On 25 March 2022, the Ministry of Economy, the IMPI and the World Intellectual Property Organization held a dialogue with micro, small and medium-sized enterprises on the importance of democratizing the use of

[559] The IFT and the CONDUSEF sign a collaboration agreement for the promotion of cybersecurity, responsible use of ICT and financial services, Mexican Government (Mexico City) 1 December 2021. Translation provided by the analyst. Access Date: 4 April 2022. https://www.gob.mx/condusef/prensa/el-ift-y-la-condusef-firman-convenio-de-colaboracion-para-la-promocion-de-la-ciberseguridad-uso-responsable-de-tic-y-servicios-financieros?idiom=es/.

[560] Seminar on the Federal Law for the Protection of Industrial Property IMPI-UP, Mexican Government (Mexico City) 6 December 2021. Translation provided by the analyst. Access Date: 4 April 2022. https://www.gob.mx/impi/articulos/seminario-de-la-ley-federal-de-proteccion-a-la-propiedad-industrial-impi-up?idiom=es.

[561] U.S.-Mexico High-Level Economic Dialogue (HLED) Fact Sheet, US Department of Commerce (Washington) 13 December 2021. Access Date: 4 April 2022. https://www.commerce.gov/news/fact-sheets/2021/12/us-mexico-high-level-economic-dialogue-hled-fact-sheet.

industrial property rights to achieve diversification and commercial exposure, respecting the characteristics that make the products and services of creators unique.[562]

Mexico has taken actions in all three aspects of the commitment.

Thus, Mexico receives a score of +1.

Analyst: Irina Popova

Russia: 0

Russia has partially complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 1 November 2021, Russia and China held a meeting on cooperation in information and communication sphere. The parties discussed issues related to network security, mailing and broadband spectrum usage in neighboring regions of the two countries. The counterparts agreed on initiation of several bilateral projects in the respective sphere.[563]

On 25 November 2021, Russia and Syria held a meeting on promoting cooperation in digital sphere. The parties agreed on deepening cooperation in cybersecurity, digital infrastructure development, providing better Internet access to Syrian nationals.[564]

On 1 February 2022, the government announced launch of the state-backed application Gosklutch (Government Key) designed as to provide Russian citizens with better protection when sealing online transactions. The new application is integrated into the government-powered system Gosuslugi (Government services). Gosklutch would allow to verify the ID of potential transaction party by gathering public data and thus providing extra protection against online threats.[565]

On 16 February 2022, the Saint Petersburg University of Telecommunications (public university) announced that a new cyber defense training facility had started operating. A new facility would provide students with access to virtual training grounds mocking real cyberattacks and thus facilitate necessary skills development for cybersecurity specialists.[566]

On 4 March 2022, the Volga Region State Telecommunications and Information Technologies University announced that it would become a control station for the National Cyber Polygon. This initiative sponsored

[562] Economy, IMPI and WIPO strengthen the industrial property of MSMEs, Mexican Government (Mexico City) 25 March 2022. Translation provide by the analyst. Access Date: 4 April 2022. https://www.gob.mx/se/articulos/economia-impi-y-ompi-fortalecen-la-propiedad-industrial-de-las-mipymes-298025?idiom=es.
[563] Russia and China to discuss ICT development, Ministry of Digital Development, Connection and Mass Communication of the Russian Federation (Moscow) 1 November 2021. Translation provided by the analyst. Access Date: 01 March 2022. https://digital.gov.ru/ru/events/41348/
[564] Russia and Syria to discuss cooperation in mass media and information technologies, Ministry of Digital Development, Connection and Mass Communication of the Russian Federation (Moscow) 25 November 2021. Translation provided by the analyst. Access Date: 01 March 2022. https://digital.gov.ru/ru/events/41366/
[565] "Gosklutch" Application to Verify Users Profiles, Ministry of Digital Development, Connection and Mass Communication of the Russian Federation (Moscow) 1 February 2022. Translation provided by the analyst. Access Date: 4 April 2022. https://digital.gov.ru/ru/events/41421/
[566] Bonch Bruevich Saint Petersburg University to Open a Cyber Polygon, Ministry of Digital Development, Connection and Mass Communication of the Russian Federation (Moscow) 16 February 2022. Translation provided by the analyst. Access Date: 4 April 2022. https://digital.gov.ru/ru/events/41426/

under the federal program "Digital Economy" would facilitate cybersecurity capacity building and necessary skills development.[567]

By means of facilitating cybersecurity capacity and skills development, Russia has addressed two out of three key commitment spheres namely privacy and data protection, and security. However, no actions matching the intellectual property rights component of the commitment has been founded within the monitoring period.

Thus, Russia receives a score of 0.

Analyst: Alexander Ignatov

Saudi Arabia: 0

Saudi Arabia has partially complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 9 December 2021, the government issued a new personal data protection law. Under the new legislation, all businesses operating in the country or processing data of local residents should exercise assessment of their activities to ensure compliance with date security standards. The law also imposes fines and penalties for non-compliance up to SAR3 million (approximately USD800,000). The law came into effect on 23 March 2022.[568]

On 1 February 2022, the government presented the Digital Tourism Strategy till 2025. The Strategy includes nine projects and 31 initiatives aimed at promotion of the country's tourism industry. One of the key initiatives proposed under the Strategy is designed as to provide string basis for informed decision-making meaning building solutions that gather data and provide analytics for businesses.[569]

On 10 March 2022, the government issued the Draft Executive Regulations to facilitate implementation of the Personal Data Protection Law (PDPL) adopted in September 2021.[570] The Draft Executive Regulations aim to clarify procedures and implementation of the provisions of the PDPL and add substantive details to the PDPL.

By means of facilitating cybersecurity capacity and skills development, Saudi Arabia has addressed two out of three key commitment spheres namely privacy and data protection, and security. However, no actions matching the intellectual property rights component of the commitment has been founded within the monitoring period.

Thus, Saudi Arabia receives a score of 0.

Analyst: Alexander Ignatov

South Africa: 0

South Africa has partially complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

[567] New National Cyber Polygon Control Base would be opened in Samara, Ministry of Digital Development, Connection and Mass Communication of the Russian Federation (Moscow) 4 March 2022. Translation provided by the analyst. Access Date: 4 April 2022. https://digital.gov.ru/ru/events/41444/

[568] Saudi Arabia Issues New Personal Data Protection Law, Covington (Washington) 9 December 2021. Access Date: 4 April 2022. https://www.insideprivacy.com/privacy-and-data-security/saudi-arabia-issues-new-personal-data-protection-law

[569] Saudi Ministry of Tourism Digital Tourism Strategy Set to Accelerate Sector, Jobs, Innovation, Ministry of Tourism of the Kingdom of Saudi Arabia (Riyadh) 1 February 2022. Access Date: 4 April 2022. https://mt.gov.sa/en/mediaCenter/News/MainNews/Pages/news-1-3-01-02-2022.aspx

[570] Saudi Arabia: Draft Regulations to the PDPL in focus – Part one: Accountability and governance, Public Consultation Platform (Riyadh) 10 March 2022. Access Date: 29 August 2022. https://istitlaa.ncc.gov.sa/en/transportation/ndmo/pdpl/Documents/ΩDraft%20of%20the%20Executive%20Regulation%20of%20Personal%20Data%20Protection%20Law%20-%20MARCH%209.pdf

On 13 May 2022, the Department of Public Service and Administration has published a Determination and Directive on the Usage of Cloud Computing Services in the Public Service.[571] This provides guidelines to public bodies on the use of cloud computing services and applies to cloud services where government data is either stored or processed.

South Africa has taken strong action on privacy and data protection. However, no action regarding intellectual property rights protection and digital security has been found during the monitoring period.

Thus, South Africa receives a score of 0.

Analyst: Alexander Ignatov

Turkey: 0

Turkey has partially complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 22 November 2022, it the Cyber Security Cluster and the Presidency of Defense Industries held the country's the National Cyber Security Summit.[572]

On 6 December 2021, the Data Protection Authority (DPA) published the Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism; in accordance with the Communiqué, (i) the trainees who have obtained the certificate of participation and who are successful in the exam will be entitled to use "data protection officer" titles, (ii) organizations accredited by the Turkish Accreditation Agency within the scope of EN ISO/IEC 17024 standard will be authorized to certify those who are successful in the relevant certification exams.[573]

On 11 January 2022, the DPA published Draft Guidelines on Cookies, which provide the definition of cookies and types of cookies (categorizing them based on timeframes, purpose and parties), assess the legal basis on the application of the PD law for processing of personal data through the use of cookies and set out conditions for such processing (explicit consent obtained, cases when explicit consent is not required, lawful consent, liability, inter alia).[574]

On 15 February 2022, the DPA published the guidance on technical and administrative measures to be taken by data controllers, in order to prevent data breaches and decrease the possible negative consequences against increased data breaches.[575]

Turkey has taken strong actions on privacy and data protection and digital security. However, no action regarding intellectual property rights protection has been found during the monitoring period.

[571] Cloud computing in the public sector, Lexology (London) 13 May 2022. Access Date: 10 June 2022. https://www.lexology.com/library/detail.aspx?g=f594e709-8ec7-4961-81cc-347606c9c0f6

[572] Number 42 Discussed at National Cyber Security Summit, Digital Transformation Office (Ankara) 22 November 2021. Access Date: 31 March 2022. https://cbddo.gov.tr/en/news/6208/milli-siber-guvenlik-zirvesi-nde-42-sayisi-konusuldu

[573] Turkey: Personal Data Protection Authority Published The Communiqué On The Procedures And Principles Regarding The Personnel Certification Mechanism, Mondaq - Moroglu Arseven (Istanbul) 16 February 2022. Access Date: 31 March 2022. https://www.mondaq.com/turkey/data-protection/1161904/personal-data-protection-authority-published-the-communiqu-on-the-procedures-and-principles-regarding-the-personnel-certification-mechanism

[574] Turkey: Turkish Data Protection Authority's Draft Guidelines On Cookies, Mondaq - ELIG Gürkaynak Attorneys-at-Law (Istanbul) 19 January 2022. Access Date: 31 March 2022. https://www.mondaq.com/turkey/data-protection/1151854/turkish-data-protection-authority39s-draft-guidelines-on-cookies

[575] Turkey: Personal Data Protection Authority Announcement: Recommended Technical And Administrative Measures For Data Controllers, Mondaq - Deris IP Attorneys (Istanbul) 23 March 2022. Access Date: 31 March 2022. https://www.mondaq.com/turkey/data-protection/1174948/personal-data-protection-authority-announcement-recommended-technical-and-administrative-measures-for-data-controllers

Thus, Turkey receives a score of 0.

Analyst: Pavel Doronin

United Kingdom: +1

The United Kingdom has fully complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 24 November 2021, the Department for Digital, Culture, Media & Sport published "National Data Strategy Mission 1 Policy Framework: Unlocking the value of data across the economy," which offers a framework for authorities' action to set the perfect conditions to "make private and third sector data more usable, accessible and available across the UK economy." At the same time, it protects people's data rights and private enterprises' intellectual property.[576]

On 25 November 2021, the Board of Trade published a new report dedicated to opportunities digital trade "for boosting UK exports, turbocharging economic growth, and creating high-paying jobs across all parts of the UK." It will help to reduce protectionism in online trade internationally, to the benefit of UK businesses and consumers, boost wages in digital sector.[577]

On 29 November 2021, the Cabinet Office's Central Digital and Data Office has developed an algorithmic transparency standard for government departments and public sector bodies to manage risks, uphold the highest standards of transparency and accountability.[578]

On 20 January 2022, the government has launched "The Government's Help to Grow: Digital Scheme" to support smaller businesses in adopting digital technologies so they can grow. Under the scheme, "businesses can admit abatements of over GBP5,000 off the retail price of approved Digital Accounting and customer relationship management software from leading technology suppliers and access practical, specialized support and advice on how to choose the right digital technologies to boost their growth and productivity."[579]

On 8 March 2022, the Department for Digital, Culture, Media & Sport has announced to make changes to the Online Safety Bill to tackle scams and fraud, which involves requiring the largest and most popular social media platforms and search engines to prevent paid-for fraudulent adverts appearing on their services.[580]

On 17 March 2022, the Department for Digital, Culture, Media & Sport introduced world-first online safety laws, which include tougher and quicker criminal sanctions for tech bosses and new criminal offences for falsifying and destroying data. The "Online Safety Bill," among other things, protects children from harmful content such as pornography and limit people's exposure to illegal content.[581]

[576] National Data Strategy Mission 1 Policy Framework: Unlocking the value of data across the economy, Department for Digital, Culture, Media & Sport (London) 24 November 2021. Access Date: 17 March 2022. https://www.gov.uk/government/publications/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy

[577] Digital trade key to unlocking opportunities of the future, UK Government (London) 25 November 2021. Access Date: 7 March 2022. https://www.gov.uk/government/news/digital-trade-key-to-unlocking-opportunities-of-the-future

[578] UK government publishes pioneering standard for algorithmic transparency, Cabinet Office (London) 29 November 2021. Access Date: 18 March 2022. https://www.gov.uk/government/news/uk-government-publishes-pioneering-standard-for-algorithmic-transparency--2

[579] Government backs UK entrepreneurs with tech support and software to help them grow, UK Government (London) 20 November 2021. Access Date: 15 March 2022. https://www.gov.uk/government/news/government-backs-uk-entrepreneurs-with-tech-support-and-software-to-help-them-grow

[580] Major law changes to protect people from scam adverts online, UK Government (London) 8 March 2022. Access Date: 18 June 2022. https://www.gov.uk/government/news/major-law-changes-to-protect-people-from-scam-adverts-online

[581] World-first online safety laws introduced in Parliament, Department for Digital, Culture, Media & Sport (London) 17 March 2022. Access Date: 17 June 2022. https://www.gov.uk/government/news/world-first-online-safety-laws-introduced-in-parliament

On 28 March 2022, the Cabinet Office announced the "New digital playbook" to cut costs and support job growth. This initiative breaks down barriers for small and medium-sized businesses, urging teams to focus on offering agile and innovative digital solutions. This focus takes advantage of tender opportunities and drive job growth right across the country.[582]

On 20 April 2022, the Department for Business, Energy & Industrial Strategy has announced about reforming competition and consumer policy in order to strengthen enforcement against illegal anticompetitive conduct and create a more active pro-competitive strategy for the Competition and Markets Authority, to keep pace with the speed of digital innovation.[583]

On 27 April 2022, the Chancellor has announced a creation of the new the new GBP25 million Public Sector Fraud Authority, which cracks down on criminal gangs who rip off the taxpayer. This body will recruit leading data analytics experts and economic crime investigators to "recover money stolen from Covid support schemes."[584]

On 13 May 2022, the Department for Business, Energy & Industrial Strategy published "Civil nuclear cyber security" strategy 2022, setting out how the UK's civil nuclear sector aims to manage and mitigate evolving cyber risks over the next 5 years due to legacy challenges and adoption of new technologies.[585]

On 13 June 2022, the Department for Digital, Culture, Media & Sport published Policy paper UK's Digital Strategy, which sets out a coherent articulation of the government's ambitious agenda for digital policy. It includes a focus on: digital infrastructure, data, regulation and digital markets, and security, consolidation of the government's work to support the innovation ecosystem, including in universities and the private sector, strengthening the digital education pipeline, financing digital growth, spreading prosperity and levelling up.[586]

The United Kingdom has taken strong actions in all three dimensions. The government adopted national privacy strategy to promote privacy and improve data protection, developed mechanisms to reduce protectionism in international online trade, created an algorithmic transparency standard for government departments and public sector bodies to manage risks in digital sphere, to protect people's data rights and private enterprises' intellectual property.

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

Analyst: Elena Alekseeva

United States: +1

The United States has fully complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 19 January 2022, President Joe Biden signed the National Security Memorandum on Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems. This Memorandum implemented the cybersecurity requirements of executive order 14028 for National Security Systems (NSS) - networks across the US Government that contain classified information or are otherwise critical to military and intelligence activities. The Memorandum provides the Director of the National Security

[582] New digital playbook to cut costs and support job growth, Cabinet Office (London) 28 March 2022. Access Date: 17 June 2022. https://www.gov.uk/government/news/new-digital-playbook-to-cut-costs-and-support-job-growth
[583] Reforming competition and consumer policy, Department for Business, Energy & Industrial Strategy (London) 20 April 2022. Access Date: 17 June 2022. https://www.gov.uk/government/consultations/reforming-competition-and-consumer-policy
[584] New 'fraud squad' will crack down on criminals who steal taxpayer money, HM Treasury (London) 27 April 2022. Access Date: 17 June 2022. https://www.gov.uk/government/news/new-fraud-squad-will-crack-down-on-criminals-who-steal-taxpayer-money
[585] Civil nuclear cyber security strategy 2022, Department for Business, Energy & Industrial Strategy (London) 13 May 2022. Access Date: 17 June 2022. https://www.gov.uk/government/publications/civil-nuclear-cyber-security-strategy-2022
[586] UK's Digital Strategy, Department for Digital, Culture, Media & Sport (London) 13 June 2022. Access Date: 17 June 2022. https://www.gov.uk/government/publications/uks-digital-strategy

Agency Paul M. Nakasone, in his role as the National Manager for NSS, with enhanced insight and authorities to better safeguard these systems.[587]

On 15 March 2022, the US, the EU, India and South Africa reached agreement on a proposed "TRIPS" patent waiver for COVID-19 vaccines. The proposal would permit an "eligible" WTO member to temporarily authorize use of patented inventions necessary for COVID-19 vaccine production and supply, without the right holder's consent. An eligible member would be any developing country member that exported less than 10 per cent of world exports of COVID-19 vaccines in 2021. It could use any instrument available in law to make the authorization.[588]

On 25 March 2022, the US and the European Commission announced that they had agreed in principle on a new Trans-Atlantic Data Privacy Framework. The Framework provides for the United States put in place new safeguards to ensure that signals surveillance activities are necessary and proportionate in the pursuit of defined national security objectives, establish a two-level independent redress mechanism with binding authority to direct remedial measures, and enhance rigorous and layered oversight of signals intelligence activities to ensure compliance with limitations on surveillance activities.[589]

The United States has taken actions in all three of the areas: privacy and data protection; security; and intellectual property rights, in accordance with the relevant applicable legal frameworks.

Thus, the US receives a score of +1.

Analyst: Andrey Shelepov

European Union: +1

The European Union has fully complied with the commitment to address challenges related to privacy, data protection, security and intellectual property rights.

On 23 April 2022, the European Parliament and the Council of the European Union reached a provisional political agreement on the Digital Services Act (DSA) which sets the standards for a safer and more open digital space for users and a level playing field for companies for years to come. Under the new rules, intermediary services, namely online platforms - such as social media and marketplaces - will have to take measures to protect their users from illegal content, goods and services. The Act also provides a safer online space for users which will have better control over how their personal data are used. Users will be empowered to report illegal content online and platforms will have to act quickly, while respecting fundamental rights, including the freedom of expression and data protection. Recipients of digital services will have a right to seek redress for any damages or loss suffered due to infringements by platforms[590]. On 16 June Parliament's Internal Market Committee endorsed the provisionally reached agreement with EU governments on the DSA.[591]

[587] Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, The White House (Washington) 19 January 2022. Access Date: 1 April 2022. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

[588] Breakthrough on a Potential COVID-19 Intellectual Property Rights Waiver, Congressional Research Service (Washington) 25 March 2022. Access Date: 20 June 2022. https://crsreports.congress.gov/product/pdf/IN/IN11901.

[589] United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework, The White House (Washington) 25 March 2022. Access Date: 1 April 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/united-states-and-european-commission-joint-statement-on-trans-atlantic-data-privacy-framework/.

[590] Digital Services Act: agreement for a transparent and safe online environment, European Parliament (Strasbourg) 23 April 2022. Access Date: 18 June 2022. https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment

[591] Internal Market Committee endorses agreement on Digital Services Act, European Parliament (Strasbourg) 16 June 2022. Access Date: 18 June 2022. https://www.europarl.europa.eu/news/en/press-room/20220613IPR32814/internal-market-committee-endorses-agreement-on-digital-services-act

On 10 May 2022, the Council of the European Union presidency and the European Parliament reached a provisional agreement on the Digital Operational Resilience Act (DORA), which will make sure the financial sector in Europe is able to maintain resilient operations through a severe operational disruption.[592] DORA sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide services related to ICT (Information Communication Technologies), such as cloud platforms or data analytics services. DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats.[593]

On 11 May 2022, the European Commission adopted a new European strategy for a Better Internet for Kids (BIK+) which sets out the vision for a Digital Decade for children and youth, based on three key pillars: safe digital experiences, protecting children from harmful and illegal online content; digital empowerment so that children acquire the necessary skills and competences; active participation, respecting children by giving them a say in the digital environment, with more child-led activities to foster innovative and creative safe digital experiences[594].

On 11 May the Commission proposed a new legislation to prevent and combat child sexual abuse online. The proposed rules will oblige providers to detect, report and remove child sexual abuse material on their services. Providers will need to assess and mitigate the risk of misuse of their services and the measures taken must be proportionate to that risk and subject to robust conditions and safeguards.[595]

On 11 May 2022, the Council of the European Union agreed on a negotiating mandate for the 2030 policy programme "Path to the Digital Decade."[596] The text aims to strengthen the EU's digital leadership promoting inclusive and sustainable digital policies that serve citizens and businesses. It provides in particular the addressing the major shortage of cybersecurity skills in the EU workforce, as an important component of protecting the EU against cyber threats. Therefore, in addition to the target on basic digital skills established in the European Pillar of Social Rights Action Plan, the EU shall have a target of 20 million employed Information and Communication Technologies specialists in the EU. One of the general objections of the plan is to ensure that democratic life, public services and health and care services are accessible online for everyone, in particular disadvantaged groups including persons with disabilities, offering inclusive, efficient and personalised services and tools with high security and privacy standards.[597]

[592] DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats, Council of the European Union (Brussels) 11 May 2022. Access Date: 18 June 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/

[593] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 COM(2020) 595 final, European Commission (Brussels) 24 September 2020. Access Date: 18 June 2022. https://data.consilium.europa.eu/doc/document/ST-11051-2020-INIT/en/pdf

[594] Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+) COM/2022/212 final, European Commission (Brussels) 15 May 2022. Access Date: 18 June 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN

[595] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse COM/2022/209 final, European Commission (Brussels) 11 May 2022. Access Date: 18 June 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472

[596] 2030 policy programme 'Path to the Digital Decade': the Council adopts its position, the Council of the European Union (Brussels) 11 May 2022. Access Date: 18 June 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/programme-d-action-a-l-horizon-2030-la-voie-a-suivre-pour-la-decennie-numerique-le-conseil-adopte-sa-position/

[597] Proposal for a Decision of the European Parliament and of the Council establishing the 2030 Policy Programme "Path to the Digital Decade" COM (2021) 574 final, European Commission (Brussels) 15 September 2021. Access Date: 18 June 2022. https://data.consilium.europa.eu/doc/document/ST-11900-2021-INIT/en/pdf

On 13 May 2022, the European Parliament and the Council of the European Union reached an agreement on measures for a high common level of cybersecurity across the Union, to further improve the resilience and incident response capacities of both the public and private sector and the EU as a whole.[598] The new directive, called "NIS2" replaces the directive on security of network and information systems (the NIS directive). The NIS2 will set the baseline for cybersecurity risk management measures and reporting obligations across all sectors that are covered by the directive. It sets out minimum rules for a regulatory framework and lays down mechanisms for effective cooperation among relevant authorities in each member state. It updates the list of sectors and activities subject to cybersecurity obligations, and provides for remedies and sanctions to ensure enforcement. The directive will formally establish the European Cyber Crises Liaison Organisation Network which will support the coordinated management of large-scale cybersecurity incidents.[599]

The European Union has fully complied its commitments in all three areas. The EU has adopted multiple measures and strategies for data protection as well as for cyber security, including cybersecurity measures for EU bodies, institutions and agencies, and cybersecurity measures for kids. It launched the new Fund to protect the intellectual property of SMEs support for reimbursement of fees.

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

Analyst Ksenia Dorokhina

[598] Strengthening EU-wide cybersecurity and resilience – provisional agreement by the Council and the European Parliament, European Parliament (Strasbourg) 13 May 2022. Access Date: 18 June 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

[599] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 COM/2020/823 final, European Commission (Brussels) 16 December 2020. Access Date: 17 June 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN