2022 G20 Bali Summit Final Compliance Report

Prepared by
Samraggi Hazra, Eisha Khan 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 17 November 2022 to 21 August 2023

6 September 2023

Feedback, as always, is welcome and is kept anonymous.
Please send comments to
g20@utoronto.ca

Contents

4. Digital Economy: Data Flow with Trust

"We remain committed to further enable data free flow with trust and promote cross-border data flows."

G20 Bali Leaders' Declaration

Assessment

	No Compliance	Partial Compliance	Full Compliance
Argentina			+1
Australia			+1
Brazil			+1
Canada		0	
China			+1
France		0	
Germany			+1
India			+1
Indonesia			+1
Italy			+1
Japan			+1
Korea		0	
Mexico		0	
Russia		0	
Saudi Arabia			+1
South Africa		0	
Türkiye			+1
United Kingdom		0	
United States			+1
European Union			+1
Average	+0.65 (83%)		

Background

For the first time the G20 addressed issues related to cross-border data flows in 2016 in Hangzhou. During the leaders' meeting, the G20 adopted the G20 Digital Economy Development and Cooperation Initiative in which they made a commitment to "support ICT [information and communications technology] policies that … promote the flow of information across borders," while recognizing that "applicable frameworks for privacy and personal data protection, as well as intellectual property rights, have to be respected as they are essential to strengthening confidence and trust in the digital economy."[364]

In 2017 in Dusseldorf the G20 ministers responsible for the digital economy adopted the joint declaration in which they re-affirmed the commitment made in Hangzhou in 2016 "to promote the flow of information across borders," while recognizing that "applicable frameworks for privacy and personal data protection, as well as intellectual property rights, have to be respected as they are essential to strengthening confidence and trust in the digital economy."[365] In Hamburg, the G20 leaders committed to "support the free flow of information while respecting applicable legal frameworks for privacy, data protection and intellectual property rights."[366] At the 2018 Buenos Aires Summit the G20 Digital Economy Ministers met in Salta where they adopted a joint declaration. The ministers recognized that "a thriving digital economy relies on quality, affordable, secure, accessible and inclusive digital infrastructure, an environment that supports innovation, appropriate policy frameworks, the capacity of people and businesses to adapt to digital transformations, and the free flow of information," and reiterated the necessity of "respecting applicable

[364] G20 Digital Economy Development and Cooperation Initiative, RANEPA (Moscow) 5 September 2016. Access Date: 3 February 2023. https://www.ranepa.ru/images/media/g20/2016Hangzhou/G20%20Digital%20Economy.pdf
[365] G20 Digital Economy Ministerial Conference, RANEPA (Moscow) 7 April 2017. Access Date: 3 February 2023. https://www.ranepa.ru/images/media/g20/2017hamburg/g20-digital-economy-ministerial-declaration-english-version.pdf
[366] G20 Leaders' Declaration, RANEPA (Moscow) 8 July 2017. Access Date: 3 February 2023. https://www.ranepa.ru/images/media/g20/2017hamburg/G20%20Hamburg%20leaders_%20communiqu%C3%A9.pdf

legal frameworks, and working to build consumer trust, privacy, data protection and intellectual property rights protection."[367] At the Buenos Aires G20 Leaders' meeting, the G20 leaders reaffirmed their support for "the free flow of information" and committed to "build consumer trust, privacy, data protection and intellectual property rights protection."[368]

At the 2019 Osaka Summit the G20 Trade Ministers and Digital Economy Ministers held a meeting in Tsukuba City, Japan, and adopted the Statement on Trade and Digital Economy. The ministers acknowledged that "cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development," but also noted that "the free flow of data raises certain challenges." The ministers agreed to "address challenges related to privacy, data protection, intellectual property rights, and security" as to "further facilitate data free flow and strengthen consumer and business trust."[369] In Osaka, the G20 leaders committed to tackle challenges related to "privacy, data protection, intellectual property rights, and security" as to "further facilitate data free flow and strengthen consumer and business trust."[370] The same year the Osaka Track on Data Free Flow with Trust was launched as to facilitate multilateral discussion on related issues.[371]

In 2020 the G20 Digital Economy Ministers further elaborated on issues raised in Osaka in 2019. The ministers re-affirmed that "the cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development" while acknowledging that "the free flow of data raises certain challenges, such as the protection of privacy and personal data." The ministers concluded that there is urgent need to "address these challenges, in accordance with relevant applicable legal frameworks" as to "further facilitate data free flow and strengthen consumer and business trust, without prejudice to legitimate public policy objectives."[372] In Riyadh the G20 leaders re-committed to "further facilitate data free flow and strengthen consumer and business trust."[373]

In 2021, the G20 Digital Economy Ministers in their joint Declaration agreed to continue "the discussion on data free flow with trust and cross-border data flow" while addressing the challenges related to "privacy, data protection, intellectual property rights and security, in accordance with the relevant applicable legal frameworks, including by identifying commonalities between existing approaches and instruments used to enable data to flow with trust across borders."[374] At the Rome Summit, the G20 leaders acknowledged "the importance of data free flow with trust and cross-border data flows" and committed to "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" along with promotion of work towards "identifying commonalities, complementarities and elements of convergence between existing regulatory approaches and instruments enabling data to flow with trust, in order to foster future interoperability."[375]

[367] G20 Digital Economy Ministerial Declaration, RANEPA (Moscow) 24 August 2018. Access Date: 3 February 2023. https://www.ranepa.ru/images/media/g20/2018buenosaires/g20_detf_ministerial_declaration_salta.pdf
[368] G20 Leaders' Declaration Building consensus for fair and sustainable development, RANEPA (Moscow) 1 December 2018. Access Date: 3 February 2023. https://www.ranepa.ru/images/media/g20/2018buenosaires/buenos_aires_leaders_declaration.pdf
[369] G20 Ministerial Statement on Trade and Digital Economy, RANEPA (Moscow) 9 June 2019. Access Date: 3 February 2023. https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157920.pdf
[370] G20 Osaka Leaders' Declaration, RANEPA (Moscow) 29 June 2019. Access Date: 3 February 2023. https://www.ranepa.ru/images/News_ciir/Project/G20_new_downloadings/FINAL_G20_Osaka_Leaders_Declaration.pdf
[371] Osaka Declaration on Digital Economy, RANEPA (Moscow) 25 January 2019. Access Date: 3 February 2023. https://www.ranepa.ru/images/News_ciir/Project/G20_new_downloadings/OSAKA_DECLARATION_ON_DIGITAL_ECONOMY_eng.pdf
[372] G20 Digital Economy Ministers Meeting, RANEPA (Moscow) 22 July 2020. Access Date: 3 February 2023. https://www.ranepa.ru/ciir/gruppa-dvadtsati/predsedatelstva/saudovskoe-predsedatelstvo-2020/22%20July%202020%20Digital%20Ministers%20Meeting%20Declaration.pdf
[373] G20 Riyadh Summit Leaders' Declaration, RANEPA (Moscow) 22 November 2020. Access Date: 3 February 2023. https://www.ranepa.ru/ciir/gruppa-dvadtsati/predsedatelstva/saudovskoe-predsedatelstvo-2020/G20%20Riyadh%20Summit%20Leaders%20Declaration_EN.pdf
[374] Declaration of G20 Digital Ministers Leveraging Digitalisation for a Resilient, Strong, Sustainable and Inclusive Recovery, RANEPA (Moscow) 5 August 2021. Access Date: 3 February 2023. https://www.ranepa.ru/images/media/g20/italyanskoe-predsedatelstvo-2021/DECLARATION-OF-G20-DIGITAL-MINISTERS-2021_FINAL.pdf
[375] G20 Rome Leaders' Declaration, RANEPA (Moscow) 31 October 2021. Access Date: 3 February 2023. https://www.ranepa.ru/images/media/g20/italyanskoe-predsedatelstvo-2021/G20-ROME-LEADERS-DECLARATION.pdf

In 2022, the G20 leaders committed to "further enable data free flow with trust and promote cross-border data flow" while recognizing "the importance to counter disinformation campaigns, cyber threats, online abuse, and ensuring security in connectivity infrastructure."[376]

Commitment Features

The commitment requires that the G20 member to take actions as to facilitate "data free flow with trust and promote cross-border data flow."

Regarding the terms used to formulate the commitment under consideration, we refer "data" as "characteristics or information, usually numerical, that are collected through observation."[377]

Definitions of the used notions of "free flow of data" and "cross border data flow" are derived from the European Commission's concept of "free flow of non-personal data" – "unrestricted movement of data across borders and IT systems."[378]

Taking into account the commitment's context, we imply that there are two pillars upon which the G20 approach to ensuring data free flow with trust rests: 1) tackling issues related to privacy, data protection, intellectual property rights, and security; 2) identifying commonalities between existing approaches and instruments used to enable data to flow with trust across borders. To fulfil the commitment made, the G20 member must take actions related to both pillars.

Pillar 1. Tackling issues related to privacy, data protection, intellectual property rights, and security

Promoting privacy and data protection

Following the Organisation for Economic Co-operation and Development (OECD) works on privacy and data protection such as the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. these aspects – privacy and data protection – 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 collected, traded or used as part of a commercial relationship.[379] "Personal data" refers to "any information relating to an identified or identifiable individual (data subject).[380]

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;

[376] G20 Bali Leaders' Declaration, G20 Information Centre (Toronto) 16 November 2022. Access Date: 3 February 2023. http://www.g20.utoronto.ca/2022/221116-declaration.html

[377] OECD Glossary of Statistical Terms: Data, OECD (Paris) 8 March 2006. Access Date: 3 February 2023. https://stats.oecd.org/glossary/detail.asp?ID=532.

[378] Free flow of non-personal data, European Commission (Brussels) 28 May 2019. Access Date: 28 February 2023. https://digital-strategy.ec.europa.eu/en/library/free-flow-non-personal-data

[379] Consumer Data Rights and Competition – Background note, OECD (Paris) 2013. Access Date: 3 February 2023. https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf

[380] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (Paris) 2013. Access Date: 3 February 2023. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

- 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.[381]

Ensuring security

According to the OECD "digital security" refers to "economic and social aspects of cybersecurity as opposed to purely technical aspects and those related to criminal law enforcement and national and international security."[382] 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."[383]

Ensuring the digital security requires cooperation of all "stakeholders" considered as "the governments, public and private organizations, and the individuals, who rely on the digital environment for all or part of their economic and social activities."[384]

To comply with this commitment feature the G20 should lead by example in implementation of a holistic public policy approach to digital security risk management and establishing co-ordination mechanisms at the domestic, regional and international levels, which ensure that all stakeholders understand digital security risk and how to manage it, take responsibility for the management of digital security, manage digital security risk in a transparent manner; 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 co-ordination mechanisms among all relevant governmental actors to ensure that their management of digital security risk is compatible and enhances economic and social prosperity;
- Ensuring the establishment of one or more Computer Security Incident Response Team (CSIRT), also known as Computer Emergency Response Team, 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;

[381] The OECD Privacy Framework, OECD (Paris) 2013. Access Date: 3 February 2023. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[382] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: 3 February 2023. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf

[383] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: 3 February 2023. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf

[384] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: Access Date: 3 February 2023. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf

- Encouraging the use of international standards and best practices on digital security risk management, and promoting their development and review through open, transparent and multistakeholder 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.[385]

Enforcing intellectual property rights

Following the World Intellectual Property Organization's (WIPO) Handbook, we understand the "intellectual property rights" (IPR) as "the legal rights which result from intellectual activity in the industrial, scientific, literary and artistic fields." WIPO also specifies that these laws "aims at safeguarding creators and other producers of intellectual goods and services by granting them certain time-limited rights to control the use made of those productions."[386]

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.

Pillar 2. Identifying commonalities between existing approaches and instruments

Pillar 2 of the commitment focuses on promotion of the G20 international cooperation on the issues related to privacy and data protection; ensuring security; and enforcing intellectual property rights. As to match this component, the G20 member shall engage in activities involving other members or promote cooperation with non-the G20 members.

Forms that the G20 member's actions might take include but not limited to:

- Organizing or participating in issue-specific meetings, seminars and workshops;
- Engaging in bilateral and multilateral negotiations on related issues;

[385] Digital Security Risk Management for Economic and Social Prosperity, OECD (Paris) 2015. Access Date: Access Date: 3 February 2023. https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf
[386] WIPO Intellectual Property Handbook, WIPO (Geneva) 2004. Access Date: 3 February 2023. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_489.pdf

- Adopting relevant amendments to national legislation following agreements achieved on international fora;

- Declaration of intent or expression of public support for multilateral initiatives in the sphere under consideration, etc.

As to achieve the full compliance or a +1 score, the G20 member shall take strong actions related to at least two out of three key spheres of the Pillar 1 and at least some of these actions must be international by nature, e.g. involving other G20 members or non-G20 states. Partial compliance or a "0" score is awarded if the G20 member takes actions (either strong or weak) that correspond with less than two Pillar 1 spheres regardless their national or international essence. A 0 score must be also given if the G20 member's actions match all three Pillar 1 spheres but not a single action is considered to be international by nature or in a case when the G20 member takes only weak actions corresponding with the Pillar 1 issues even if they involve a foreign state or a group of states. Non-compliance or a −1 score is awarded if the G20 member takes not a single action corresponding with any of the Pillar 1 spheres. Strong action in this context implies that the G20 member's actions go beyond mere verbal support or participation in a discussion on a topic without further implementation in a legislative form, resources allocation, entering a formal bilateral or multilateral agreement, etc.

Scoring Guidelines

−1	G20 member does no action addressing challenges such as those related to privacy and data protection; security; and intellectual property rights
0	G20 member takes actions in ANY of the Pillar 1 areas: privacy and data protection; security; and intellectual property rights, BUT not a single action could be considered to be international OR all the actions taken are considered weak
+1	G20 member takes strong actions corresponding with at least TWO of the Pillar 1 areas: privacy and data protection; security; and intellectual property rights AND at least ONE sphere is supported with a strong international action

Compliance Director and Lead Analyst: Alexander Ignatov

Argentina: +1

Argentina has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

In February 2023, the Agency for Access to Public Information (AAIP) published on its website a new version of the project that seeks to replace Law 25,326 on the Protection of Personal Data with new modifications compared to the November 2022 version.[387] It incorporates credit entities (with a specific definition) as active subjects in the diligent disclosure of people's credit information, being those in charge of transferring this information to the Central Bank of the Argentine Republic for its publication, as well as how to keep it updated and respond to any challenge. In order to harmonize data processing with information on human rights violations (the so-called memory, truth and justice process, the AAIP), the new version of the bill clarifies that the clarification of serious cases of human rights violations human rights and crimes against humanity are exceptions to the prohibition of the processing of sensitive data and to the exercise of the right of deletion.

On 16 February 2023, Minister of Security Aníbal Fernández signed Argentina's adherence to the Second Additional Protocol of the Budapest Convention of the European Union, on cybercrime, a tool that will reduce the time for investigations of cybercrime at the international level.[388]

On 28 February 2023, head of the AAIP Beatriz de Anchorena participated in the meeting organized by the Spanish Agency for Data Cooperation, the Ibero-American Network for Data Protection and the

[387] Ley De Protección De Datos Personales, Agencia de Acceso a la Información Pública (Buenos Aires) February 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_proteccion_de_datos_personales_-_febrero_2023.pdf.
[388] Argentina and France strengthen security cooperation ties, Government of Argentina (Buenos Aires) 28 February 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.argentina.gob.ar/noticias/argentina-y-francia-fortalecen-los-lazos-de-cooperacion-en-materia-de-seguridad.

Spanish Agency for International Development Cooperation.[389] In the first part of the meeting, the members of the Network worked on the new legislative developments of the Ibero-American Data Protection Network and discussed the importance of updating the Personal Data Law of the Argentine Republic, promoted by the AAIP, to respond to the new challenges imposed by technological transformations and the development of the digital economy. The second panel focused on the Argentine experience regarding the current model contractual clauses for the international transfer of personal data (Provision 60/2016) in relation to the clauses established in the Ibero-American Network for the Protection of Personal Data. These clauses are a guarantee instrument for the protection of personal data in cross-border flows, when a country does not have adequate legislation for international transfers. The Agency for Access to Public Information is the one that evaluates the level of protection provided by these regulations at the national level.

On 6 March 2023, Minister of Security Fernández and governor of the province of Formosa Gildo Insfrán led the opening of the conference "ForCIC BOOTCAMPs," as part of the cybercrime training promoted by this Ministry in the framework of the Cybersecurity and Cybercrime Investigation Strengthening Program.[390]

On 10 March 2023, the Central Bank of Argentina updated the technology and information security risk standards by issuing Communication 'A' 7724 in order to strengthen the capacity of financial institutions to withstand cyber threats by introducing new minimum requirements for the management and control of information technology and security.[391] The aforementioned addition is aimed at the creation of departments and positions for managers that would control cyber risks, classify data and information, develop a backup technology inside institutions to ensure availability of data and, additionally, promote security on e-commerce platforms and social networks by identifying and deleting unauthorised profiles.

On 30 March 2023, the second meeting of the "Data Governance and Privacy Protection" commission of the Federal Council for transparency was held.[392] This meeting was part of a series of meetings within the commission's work plan. The meeting was focused on the protection of personal data and included the participation of representatives of the Council, members of the Commission and AAIP authorities. Constituted by the 24 jurisdictions of our country through Law 27,275, the Federal Council for Transparency is the permanent interjurisdictional body whose purpose is technical cooperation and the coordination of policies on transparency, access to public information and the personal data protection.

On 17 April 2023, Argentina became the 23rd country to ratify the amending protocol to the Convention 108 with the Director of the Agency of Access to Public Information of Argentina, Beatriz de Anchorena depositing the documents handed over the ratification documents during the 2023 Privacy Symposium under the special programme on the basis of the Council of Europe.[393]

[389] Ibero-American Meeting on Data Protection 2023, Government of Argentina (Buenos Aires) 28 February 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.argentina.gob.ar/noticias/encuentro-iberoamericano-de-proteccion-de-datos-2023.

[390] In Formosa, Aníbal Fernández and Gildo Insfrán inaugurated training sessions on cybercrime for seven provinces, Government of Argentina (Buenos Aires) 6 March 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.argentina.gob.ar/noticias/en-formosa-anibal-fernandez-y-gildo-insfran-inauguraron-jornadas-de-capacitacion-en.

[391]Argentina: Minimum requirements for management and control of IT and security risks, Baker McKenzie 1 April 2023. Access Date: 20 June 2023 https://www.globalcompliancenews.com/2023/04/01/argentina-minimum-requirements-for-management-and-control-of-it-and-security-riskshttps-insightplus-bakermckenzie-com-bm-technology-media-telecommunications_1-argentina-central-bank-communication-a/

[392] Second meeting of the "Data Governance and Privacy Protection" commission of the Federal Council for Transparency, Government of Argentina (Buenos Aires) 30 March 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.argentina.gob.ar/noticias/segunda-reunion-de-la-comision-gobernanza-de-datos-y-proteccion-de-la-privacidad-del.

[393]Privacy Symposium examines global role of data protection convention; Argentina ratifies amending protocol, Council of Europe 17 April 2023. Access Date: 18 June 2023 Argentina ratifies amending protocol - Le Conseil de l'Europecoe.int https://www.coe.int › portal

On 22 April 2023, the Agency for Access to Public Information presented the Bill of Law on Personal Data Protection, that is aimed at updating of Data Protection Law 25,326.[394] The project introduced new requirements for the legal bases for data processing, which states that prior to the usage of the data, the detailed and documented analysis must be presented to determine the legitimacy of interest.

On 27 April 2023, the Government published the report on the conference "Optimicemos la Ciberseguridad" ("Let's optimise cybersecurity"), during which Undersecretary of Information Technologies Agustina Brizio, Deputy Executive Secretary of the International Counter-Terrorism Committee of the Organization of American States Violanda Botet and Country Manager of Amazon Web Services in Argentina Lorena Zicke presented an overview of the current advances of cybersecurity in Argentina, in which the progress of the Second National Cybersecurity Strategy was highlighted.[395] By this, Argentina not only provided the updates on the data and cybersecurity, but also promoted cooperation.

On 30 June 2023, the National Executive Branch send out Message 87/2023 to the Honorable Chamber of Deputies of the Nation with the Personal Data Protection Bill of Law, which was updated as a response to the new concerns and suggestions of experts, citizens and representatives and is aimed at harmonisation of local standards with regional and international ones in the times of technological transformation.[396]

In July 2023, the Agency for Access to Public Information (AAIP) approved Program on Transparency, Document Management and Archives, as well as 2022-2026 Strategic Plan.[397] The first document, marked as Resolution AAIP 93/2023, consists of two main areas, the first being dedicated to facilitation of the access to public information and improvement of the quality of produced information and the transparency of the obligated subjects in the exercise of their power, while the second part aims at achieving consensus to balance between broad access to information and the protection of that information. Resolution AAIP 94/2023, or Strategic Plan for the period 2022-2026, has set four objectives is aimed at promotion and strengthening of the right to the protection of personal data and access to public information, as well as the institutional powers of the AAIP.

Argentina has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows. Argentina has taken strong actions on further enable data free flow with trust and promote cross-border data flows through data protection and cybersecurity, including through international cooperation.

Thus, Argentina receives a score of +1.

Analysts: Irina Popova and Victoria Mushina

Australia: +1

Australia has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 17 November 2022, Australia and India convened their fifth Bilateral Cyber Policy Dialogue in New Delhi. The dialogue was co-chaired by Joint Secretary (Cyber Diplomacy Division) Ms. Muanpuii Saiawi

[394] Argentina: The Agency for Access to Public Information announced the presentation of the Bill of Law on Personal Data Protection in the National Congress, Baker McKenzie 22 April 2023. Access Date: 20 June 2023 https://www.globalcompliancenews.com/2023/04/22/https-insightplus-bakermckenzie-com-bm-technology-media-telecommunications_1-argentina-the-agency-for-access-to-public-information-announced-the-presentation-of-the-bill-of-law-on-personal-data-prot/

[395]The conference "Optimize Cybersecurity" was held together with the OAS and AWS, Government of Argentina (Buenos Aires) 27 April 2023. Translation provided by the analyst. Access Date: 21 June 2023 https://www.argentina.gob.ar/noticias/se-desarrollo-la-jornada-optimicemos-la-ciberseguridad-junto-la-oea-y-aws

[396]Argentina: National Executive Branch submits Bill of Law on Personal Data Protection to Congress, Baker McKenzie 11 July 2023. Access Date: 7 August 2023 https://www.globalcompliancenews.com/2023/07/11/https-insightplus-bakermckenzie-com-bm-investigations-compliance-ethics-argentina-national-executive-branch-submits-bill-of-law-on-personal-data-protection-to-congress_07042023/

[397] Argentina: Agency for Access to Public Information approves Program on Transparency, Document Management and Archives and its 2022-2026 Strategic Plan. Baker McKenzie 10 July 2023. Access date: 16 July 2023https://insightplus.bakermckenzie.com/bm/data-technology/argentina-agency-for-access-to-public-information-approves-program-on-transparency-document-management-and-archives-and-its-2022-2026-strategic-plan

from Ministry of External Affairs of the Government of India and Dr. Tobias Feakin, Ambassador for Cyber Affairs and Critical Technology, Department of Foreign Affairs and Trade, Government of Australia. The Cyber Policy Dialogue was held under the auspices of the India-Australia Framework Arrangement on Cyber and Cyber-Enabled Critical Technology Cooperation and Plan of Action 2020-2025 for a comprehensive and deeper cyber cooperation.[398]

On 24 November 2022, the Government released the Essential Eight Assessment Guidance Package – a comprehensive guideline designed as to support entities to gather and test system configurations to mitigate cybersecurity risks. Government approved resources are said to enable "a high quality, consistent approach for entities to assess the effectiveness of their implementation of the Essential Eight security controls." The guidance includes a special toolbox that would help entities assess their maturity level in line with the abovementioned strategies.[399]

On 25 November 2022, the Government announced that it would invest AUD25.4 million as to "improve the quality, quantity and diversity of Australia's cybersecurity workforce." 18 projects were selected as recipients of the funding. The selected projects target some of vulnerable and underrepresented groups including women, First Nations Australians, remote area dwellers, and people with neurodiverse background.[400]

On 1 December 2022, the Government established the Cyber Security Response Coordination Unit. The unit would work with the relevant agencies across the Commonwealth to 'lead technical incident responses, law enforcement operations, and regulatory activities'.[401]

On 16 December 2022, the Cyber Security Centre released a guideline to help small business establish more secure cloud environment and thus protect themselves from the most common types of cyber accidents.[402] The guideline is designed as being applicable to any type of small enterprise even those having no sufficient resources necessary to provide essential level of protection.

On 7 February 2023, the Quad partners of Australia, India, Japan, and the United States are launching a public campaign to improve cyber security across our nations: the Quad Cyber Challenge. The Challenge provides resources, such as basic cybersecurity information and training, for all users – from corporations to education institutions, small businesses, and individuals from grade school students to the elderly. The Quad partners are working to ensure everyone has access to the resources needed to make informed decisions while online and using smart devices.[403]

On 9 May 2023, the Government presented the Federal Budget for the 2023 – 2024 period. The Government allocated AUD86.5 million to "establish Australia's first SMS ID Registry to prevent scammers imitating trusted brand names."[404] Also the Government grants AUD44.3 million to assist the Office of Information Commissioner in taking appropriate regulatory actions as to enhance its data and analytics capability.

[398] Fifth India-Australia Cyber Policy Dialogue, Australian Government (Canberra) 17 November 2022. Access Date: 11 April 2023. https://www.internationalcybertech.gov.au/Fifth-India-Australia-Cyber-Policy-Dialogue.
[399] The ACSC has published updated guidance to help ensure consistent Essential Eight assessment across government and industry, Australian Government Department of Industry, Science and Resources (Canberra) 24 November 2022. Access Date: 10 April 2023. https://www.cyber.gov.au/acsc/view-all-content/news/essential-eight-assessment-guidance-package
[400] Upskilling and diversifying Australia's cyber security workforce, Australian Government Department of Industry, Science and Resources (Canberra) 25 November 2022. Access Date: 10 April 2023. https://www.industry.gov.au/news/upskilling-and-diversifying-australias-cyber-security-workforce
[401] Learn more about the stand-up of the National Office for Cyber Security Exercise Program, Government of Australia Cyber and Infrastructure Security Centre (Canberra) 19 May 2023. Access Date: 28 June 2023. https://www.cisc.gov.au/news-media/archive/article?itemId=1062
[402] Small Business Cloud Security Guides, Australian Government Signals Directorate (Canberra) 16 December 2022. Access Date: 10 April 2023. https://www.cyber.gov.au/acsc/view-all-content/news/small-business-cloud-security-guides
[403] Quad Joint Statement on Cooperation to Promote Responsible Cyber Habits, the White House (Washington DC) 7 February 2023. Access Date: 11 April 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/02/07/quad-joint-statement-on-cooperation-to-promote-responsible-cyber-habits/.
[404] Budget 2023 – 24 Stronger foundations for a better future, Government of Australia (Canberra) 9 May 2023. Access Date: 28 June 2023. https://budget.gov.au/content/overview/download/budget_overview-20230511.pdf

Australia took strong actions that match the Pillar 1 component of ensuring cyber security by means of promoting skills development and implementation of the best available practices. Also, it has contributed to better enforcement of intellectual property rigths by working on prevention of online scamming as well as facilitation of international cooperation on data security.

Thus, Australia receives a score of +1.

Analyst: Alexander Ignatov

Brazil: +1

Brazil has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 27-28 February 2023, the National Data Protection Authority (ANPD) participated in the Ibero-American Data Protection Meeting.[405] The objective of the Brazilian participation was to expand ANPD's work with the Ibero-American Republic, providing international dialogues that favor the dissemination of the data protection culture worldwide, and also, to promote global regulatory harmonization.

On 16 March 2023, the ANPD hosted the World Bank Digital Development specialist Julian Najles for a technical meeting.[406] The meeting served to present the current structure of the ANPD and to discuss future action plans by the Authority to promote the protection of privacy and personal data in the country. Julian Najles reported on World Bank projects to foster initiatives related to the protection of personal data.

On 28-29 March 2023, Director-President of the ANPD Wal de mar Gonçalves Ortunho Júnior participated in the 38th Public Hearing of the Federal Supreme Court, convened within the scope of Extraordinary Appeals 1.037.396- SP and 1,057,258-RJ.[407] The public hearing, brought together specialists from the private and government sectors, and aims to promote discussions on the following topics: (1) the liability regime for providers of applications or tools internet for user-generated content; and (2) the possibility of removing content that may offend personality rights, incite hatred or spread fraudulent news based on extrajudicial notification.

On 4-5 April 2023, the ANPD, represented by Director Miriam Wimmer, participated in the Global Privacy Summit, held annually by the International Association of Privacy Professionals, in Washington, United States.[408] Director Wimmer discussed advances in the field of data protection in Brazil, highlighting the creation and institutional strengthening of ANPD, with its transformation into an autarchy and on the incorporation into the Brazilian Federal Constitution of the fundamental right to the protection of personal data.

On 5 April 2023, the meeting between the secretary for Policies and Strategic Programs of the Ministry of Science, Technology and Innovation (MCTI) Marcia Barbosa and Director of the Division for Latin America and the Caribbean of the World Intellectual Property Organization (WIPO) Office Beatriz Amorim-Borher took place.[409] Among the aspects of the subject addressed during the meeting was the need to encourage female participation in science, technology, engineering and mathematics (STEM) and, consequently, increase the number of women inventors. Director Borher also highlighted that the WIPO

[405] ANPD participates in the Ibero- American Data Protection Meeting, Government of Brazil (Brasilia) 28 February 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-do-encontro-ibero-americano-de-protecao-de-dados.

[406] ANPD and the World Bank meet at the Authority for, Government of Brazil (Brasilia) 16 March 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-banco-mundial-reunem-se-na-sede-autoridade.

[407] ANPD participates in a public hearing on the Civil Rights Framework for the Internet, Government of Brazil (Brasilia) 29 March 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-de-audiencia-publica-sobre-o-marco-civil-da-internet.

[408] ANPD participates for the second time in the IAPP Global Privacy Summit, Government of Brazil (Brasilia) 5 April 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-pela-segunda-vez-do-iapp-global-privacy-summit.

[409] MCTI and the World Organization for Intellectual Property study cooperation to disseminate knowledge in the area, Government of Brazil (Brasilia) 5 April 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2023/04/mcti-e-organizacao-mundial-para-propriedade-intelectual-estudam-cooperacao-para-difundir-conhecimentos-da-area.

intends to develop a specific edition with Brazil for women in STEM careers, including entrepreneurship. The MCTI is part of the Interministerial Group on Intellectual Property and has initiatives to encourage entrepreneurship, especially the participation of women and girls in science, carried out by linked units, such as Women Entrepreneurs, Future Scientists and the Centelha Program.

On 6 April 2023, to align the information security guidelines in the federal government, the Digital Government Secretariat of the Ministry of Management and Innovation in Services held a webinar with representatives of the bodies and entities of the federal public administration that make up the Information Technology Resources Management System.[410] The objective of the webinar was to disseminate the Guide to the Privacy and Information Security Framework. The guide is part of the Information Privacy and Security Program formalized by Ordinance No. 852/23, published at the end of March. The guide was developed in partnership with the United Kingdom government.

On 6 April 2023, the ANPD released a new page on its website aimed at clarifying the Impact Report on Personal Data Protection with 15 questions and answers on the topic.[411] The authority 's initiative, in addition to promoting understanding on the subject and solving possible doubts, is to better guide personal data controllers so that they can act in favor of the data security of the holders who are under their responsibility. The elaboration of Impact Report on Personal Data Protection, which is the responsibility of the controller of personal data, serves to describe the processes of processing personal data that can generate high risk to the guarantee of the general principles of protection of personal data, to freedom of civil rights and the fundamental rights of the data subject. The document should also contain measures of protection and mechanisms that can reduce risks to the protection of the holders' rights.

On 28 April 2023, the ANPD met with representatives of Human Rights Watch, an international non-governmental organization dedicated to the protection of human rights, to discuss measures to protect children and adolescents in the digital environment.[412] The organization recently published a report that investigated the collection and monitoring of data on children and adolescents by Brazilian educational platforms.

On 16 May 2023, ANPD was visited by the president of the Access to Public Information Agency of Argentina.[413] Meeting between the entities aims to establish a partnership for the exchange of experiences in the regulation of international transfers of personal data.

On 18 May 2023 the, ANPD participated in a Public Hearing at the Infrastructure Commission of the Federal Senate to address the implementation of cybernetic readiness strategies and preventive protection of government databases against eventual hacker attacks.[414]

On 24 May 2023, the ANPD published a Statement that intends to standardize the interpretation of the General Law for the Protection of Personal Data (LGPD) regarding the legal hypotheses that authorize the

[410] Ministry of Management of hoist information security guide to managers and technology teams of federal government agencies, Government of Brazil (Brasilia) 6 April 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.gov.br/governodigital/pt-br/noticias/ministerio-da-gestao-detalha-guia-de-seguranca-da-informacao-a-gestores-e-equipes-de-tecnologia-de-orgaos-do-governo-federal.

[411] ANPD publishes page with questions and answers about the Personal Data Protection Impact Report (RIPD), Government of Brazil (Brasilia) 6 April 2023. Access Date: 10 April 2023. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-pagina-com-perguntas-e-respostas-sobre-o-relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

[412] ANPD meets with Human Rights Watch to address the protection of personal data of children and adolescents, Government of Brazil (Brasilia) 28 April 2023. Access date: 29 June 2023. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-reune-se-com-a-human-rights-watch-para-tratar-da-protecao-de-dados-pessoais-de-criancas-e-adolescentes.

[413] ANPD welcomes president of the Access to Public Information Agency of Argentina, Government of Brazil (Brasilia) 16 May 2023. Access date: 29 June 2023. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-recebe-presidente-da-agencia-de-acesso-a-informacao-publica-da-argentina.

[414] ANPD participates in debate in the Federal Senate on hacker attacks on government networks, Government of Brazil (Brasilia) 18 May 2023. Access date: 29 June 2023. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-de-debate-no-senado-federal-sobre-ataques-de-hackers-em-redes-do-governo.

processing of data of children and adolescents.[415] The measure represents the first initiative of the ANPD related to the protection of personal data of children and adolescents and establishes the Authority's understanding of the interpretation possibilities of article 14 of the LGPD. According to the Statement, the processing of personal data of children and adolescents can be carried out based on the legal hypotheses provided for in the LGPD, such as in cases of consent provided by the holder, compliance with a legal obligation, protection of life or service to legitimate interest of the controller. In any situation, the best interest of the child and adolescent must prevail, requiring careful evaluation by the controller.

On 24-26 May 2023, the ANPD participated in Computer, Privacy and Data Protection – CPDP 2023" conference, international conference is one of the world's leading data protection and privacy events.[416] General Coordinator of Institutional and International Relations of ANPD Juliana Müller participated in the panel "What will change in 2024." She spoke about the reasons that led the ANPD to apply as an observer country of the convention and about the advantages of Brazil's possible accession to Convention 108+. Created by the Council of Europe, on January 28, 1981, Convention 108 deals with the Protection of Natural Persons with regard to Automated Processing of Personal Data. It was the first legally binding international instrument adopted in the field of data protection.

Brazil has taken strong actions to further enable data free flow with trust and promote cross-border data flows on data protection and intellectual property rights, including through international cooperation.

Thus, Brazil receives a score of +1.

Analyst: Irina Popova

Canada: 0

Canada has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 20 December 2022, Minister of Sport and Minister responsible for the Economic Development Agency of Canada for the Regions of Quebec Pascale St-Onge highlighted the benefits of the Canada Digital Adoption Program's Grow Your Business Online grant for small businesses in Quebec.[417] As part of the grant, small businesses would also receive advice from e-commerce advisors, noted that small businesses can access a grant of up to CAD2,400 to help them adopt e-commerce or expand existing e-commerce operations. As part of the grant, small businesses would also receive advice from e-commerce advisors.

On 30 January 2023, the Office of the Privacy Commissioner of Canada (OPC) has provided the Joint Chairs of the Special Joint Committee on the Declaration of Emergency with an overview of the principles that government institutions should adhere to during an emergency to ensure that privacy rights are respected.[418] The brief also outlines issues the OPC is examining in the context of files related to the disruptions, blockades and occupation that took place in February 2022.

[415] ANPD publishes statement on the processing of personal data of children and adolescents, Government of Brazil (Brasilia) 24 May 2023. Access date: 29 June 2023. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes.
[416] ANPD participates in CPDP 2023, Government of Brazil (Brasilia) 26 May 2023. Access date: 29 June 2023. Translation provided by the analyst. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-da-cpdp-2023.
[417] Minister St-Onge highlights benefits of Canada Digital Adoption Program for small businesses in Quebec, Government of Canada (Ottawa) 20 December 2022. Access Date: 30 March 2023 https://www.canada.ca/en/innovation-science-economic-development/news/2022/12/minister-st-onge-highlights-benefits-of-canada-digital-adoption-program-for-small-businesses-in-quebec.html
[418] Commissioner submits brief at request of Special Joint Committee on the Declaration of Emergency, The Privacy Commissioner of Canada (Ottawa) 30 January 2023. Access Date: 30 March 2023 https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230130/

On 8 February 2023, Minister of Innovation, Science and Industry François-Philippe Champagne launched the third phase of the Digital Skills for Youth program and highlighted a CAD10.68 million federal investment in the program.[419]

On 22 February 2023, Minister of Rural Economic Development Gudie Hutchings and Member of Parliament for Avalon Ken McDonald together with Minister of Digital Government Sarah Stoodley announced up to CAD94 million in federal and provincial funding for Bell and Xplore to bring high-speed Internet access to over 36,000 homes in over 350 rural, remote and indigenous communities across the province.[420]

On 23 February 2023, Minister of Public Safety Marco Mendicino, announced new funding for two innovative cybersecurity projects at the Université de Sherbrooke.[421] Supported by CAD1.9 million in federal funding from the Cyber Security Cooperation Program, they will help keep Canadians safe online. Both projects will enhance critical infrastructure protection in Canada. The first, Evaluation of the resilience of an electrical redistributor in an Industry 4.0 context, focuses on protection of the electrical grid, particularly smaller electricity providers. The second, Security in the Industrial Internet of Things in a context of 5G connectivity and edge processing focuses on cyber security in the integration of service providers in a 5G wireless environment.

On 29 March 2023, Privacy Commissioner Philippe Dufresne has provided Minister Champagne with recommendations to ensure that privacy considerations are factored into potential reforms of Canada's national competition policy.[422] The submission follows the release of Innovation, Science and Economic Development Canada's discussion paper and its consultation on the Future of Competition Policy in Canada, which seeks feedback on potential legislative changes to the Competition Act. The submission highlights the growing intersection between privacy and competition, and how changes to competition legislation may have effects on consumer privacy.

On 4 April 2023, the Office of the Privacy Commissioner launched an investigation into the company behind artificial intelligence-powered chatbot ChatGPT in response to a complaint alleging the collection, use and disclosure of personal information without consent.[423]

On 6 June 2023, the Office of the Privacy Commissioner of Canada has signed a renewed Memorandum of Understanding (MoU), with a goal of promoting cross-border cooperation to combat unsolicited communications, including spam, scams, and telemarketing.[424] The MoU has also been signed by the Canadian Radio-television and Telecommunications Commission (CRTC) and regulatory agencies from Australia, South Korea, the Netherlands, the United Kingdom, and New Zealand.

On 12 July 2023, Minister of Public Services and Procurement Helena Jaczek together with Member of Provincial Parliament for Markham–Stouffville Paul Calandra announced CAD54 million in combined

[419] Government of Canada helps youth build the digital skills they need for the evolving digital economy, Government of Canada (Ottawa) 8 February 2023. Access Date: 30 March 2023 https://www.canada.ca/en/innovation-science-economic-development/news/2023/02/government-of-canada-helps-youth-build-the-digital-skills-they-need-for-the-evolving-digital-economy0.html

[420] Governments of Canada and Newfoundland and Labrador invest up to $94 million to bring high-speed Internet to more than 36,000 homes in over 350 communities across the province, Government of Canada (Ottawa) 22 February 2023. Access Date: 30 March 2023 https://www.canada.ca/en/innovation-science-economic-development/news/2023/02/governments-of-canada-and-newfoundland-and-labrador-invest-up-to-94million-to-bring-high-speed-internet-to-more-than-36000homes-in-over-350communit.html

[421] Government announces new funding for research projects to enhance cyber security, Government of Canada (Ottawa) 23 February 2023. Access Date: 30 March 2023 https://www.canada.ca/en/public-safety-canada/news/2023/02/government-announces-new-funding-for-research-projects-to-enhance-cyber-security.html

[422] Commissioner submits recommendations on reforming the Competition Act, The Privacy Commissioner of Canada (Ottawa) 29 March 2023. Access Date: 30 March 2023 https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230329/

[423] OPC launches investigation into ChatGPT, The Canadian Government 4 April 2023 Access Date: 27 June 2023 https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/

[424] OPC signs agreement to promote cross-border cooperation on combatting unsolicited communications and scams, The Canadian Government 6 June 2023 Access Date: 27 June 2023 https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230606/

federal and provincial funding for Rogers Communications to bring high-speed Internet access to more than 20,000 homes in 83 underserved communities in Ontario.[425] The announcement brings the Government of Ontario closer to achieving its goal of bringing reliable high-speed Internet access to every community by the end of 2025.

Canada has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows. Canada has taken steps to ensure better data protection and security, but no action aimed at better enforcement of intellectual property rights has been found.

Thus, Canada receives a score of 0.

Analyst: Nikita Shilikov

China: +1

China has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 8 December 2022, the Ministry of Industry and Information Technology (MIIT) released the final version of the Interim Administrative Measures for Data Security in Industry and Information Technology (Measures) after two rounds of public consultation, which became the first sectoral regulation on the data security regime that the Data Security Law proposed to establish.[426]

On 13 December, the MIIT issued the Measures for the Administration of Data Security in the Field of Industry and Information Technology (for Trial Implementation), with effect from 1 January 2023.[427] The Measures focus on the following four aspects: (1) the management of data classification and grading, as well as the identification and filing of important and core data; (2) requirements for security management and protection of the lifecycle processing of data of various grades; (3) monitoring and early warning of data security threats, reporting and sharing of risk information, emergency response, the acceptance of complaints and reports, as well as other working mechanisms; and (4) monitoring, certification, and evaluation of data security.

On 16 December 2022, the secretariat of the National Information Security Standardization Technical Committee issued the Network Security Standard Practice Guide – Security Certification Specification for Cross-border Personal Information Processing Activities V2.0.[428] The Practice Guide stipulates the basic principles to be followed in cross-border processing of personal information and the relevant obligations and responsibilities of data processors and foreign recipients in the protection of the rights and interests of data subjects.

On 30 December 2022, the China Banking and Insurance Regulatory Commission issued the Administrative Measures for the Protection of Consumer Rights and Interests by Banking and Insurance Institutions, which will come into force on 1 March 2023.[429] The Administrative Measures primarily consist

[425] Governments of Canada and Ontario invest $54 million to bring high-speed Internet access to more than 20,000 homes, The Canadian Government (Ottawa) 12 July 2023 Access Date: 24 August 2023 https://www.canada.ca/en/innovation-science-economic-development/news/2023/07/governments-of-canada-and-ontario-invest-54-million-to-bring-high-speed-internet-access-to-more-than-20000-homes.html

[426] China to Strengthen Data Security in Industry and IT Sectors, Bird&Bird (Beijing) 8 December 2022. Access Date: 11 April 2023. https://www.twobirds.com/en/insights/2023/china/china-to-strengthen-data-security-in-industry-and-it-sectors.

[427] Notice of the Ministry of Industry and Information Technology on Printing and Distributing the "Data Security Management Measures in the Field of Industry and Information Technology (Trial)", Ministry of Industry and Information Technology of China (Beijing) 13 December 2022. Access Date: 11 April 2023. Translated by Google translate. https://www.miit.gov.cn/jgsj/waj/wjfb/art/2022/art_e4d9ba53a8014d85a4f80d47272f486d.html.

[428] Notice on Issuing the "Practice Guidelines for Network Security Standards - Security Certification Specifications for Cross-Border Processing of Personal Information V2.0", National Information Security Standardization Technical Committee of China (Beijing) 16 December 2022. Translation provided by Google translate. Access Date: 11 April 2023. https://www.tc260.org.cn/front/postDetail.html?id=20221216161852.

[429] The China Banking and Insurance Regulatory Commission issued the "Administrative Measures for the Protection of Consumer Rights and Interests of Banking and Insurance Institutions", China Banking and Insurance Regulatory Commission (Beijing) 30 December 2022. Translation provided by Google Translate. Access Date: 11 April 2023. http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=1087560&itemId=915.

of five parts: (1) provisions on the overall objectives, the definition of banking and insurance institutions, their responsibilities and obligations, the supervisory organisation, and the basic principles; (2) the system and mechanism for protecting consumer rights and interests; (3) rules governing the operation of banking and insurance institutions to protect the basic rights of consumers; (4) the supervision and management of the industry; and (5) the scope of application, the power of interpretation, and the timeframe for implementation.

On 21 February 2023, China presented its Global Security Initiative Concept Paper. It calls on other countries to deepen international cooperation in the field of information security.[430] It mentions that China put forward the Global Initiative on Data Security and called for joint efforts to formulate global rules on digital governance that reflect the will and respect the interests of all parties. It also gives examples of an existing initiatives put forward by China: the China-LAS Cooperation Initiative on Data Security and the Data Security Cooperation Initiative of China+Central Asia. They help to address various cyber threats, and work to establish a global governance system on cyberspace featuring openness and inclusion, justice and fairness, security and stability, vigor and vitality.

On 25 April 2023, the National Copyright Administration and the World Intellectual Property Organization signed an updated memorandum of understanding to deepen bilateral cooperation.[431] The updated MoU aims to consolidate the existing exchanges and cooperation in the field of copyright and expand the bilateral cooperation in formulating and implementing international copyright treaties, discussing digital copyright protection issues, improving the risk prevention and control capacity of the copyright industry, sharing copyright to encourage creation and innovation among the small- and medium-sized enterprises, and promoting the inheritance and development of folk literature and art.

On 26 April 2023, the national parliament voted to adopt a revised Counter-Espionage Law, which will take effect on 1 July 2023.[432] The revised law refines the definition of espionage, specifying acts such as carrying out cyber attacks against state organs, confidential organs or crucial information infrastructure as acts of espionage.

On 23 May 2023, State Councilor and Foreign Minister Qin Gang held talks with Dutch Deputy Prime Minister and Foreign Minister Wopke Hoekstra.[433] Noting that the Netherlands is an important partner of China in Europe, Qin said that China is willing to strengthen economic, trade and investment cooperation, deepen cultural and people-to-people exchanges, and advance multilateral cooperation in arms control, cyber security and climate change with the Netherlands. It was also claimed that China will continue to expand market access and strengthen intellectual property rights protection.

On 2 June 2023, the State Council executive meeting chaired by Premier Li Qiang announced that China will roll out more targeted and effective measures to improve its business environment at a faster pace, in an effort to bolster economic recovery.[434] The measures will focus on fair competition, intellectual property rights protection, a unified market and easing market access, the meeting said.

China has taken strong actions on data protection and cybersecurity, including through international cooperation. China has introduced amendments to security laws to properly manage cyberthreats, enforced coherence with international intellectual property rights standards, and presented new ruling to facilitate consumer protection in the insurance services market.

Thus, China receives a score of +1.

[430] The Global Security Initiative Concept Paper, Ministry of Foreign Affairs of People's Republic of China (Beijing) 21 February 2023. Access Date: 11 April 2023. https://www.fmprc.gov.cn/mfa_eng/wjbxw/202302/t20230221_11028348.html.
[431] China deepens cooperation with World Intellectual Property Organization, News.cn (Beijing) 25 April 2023. Access date: 29 June 2023. https://news.cgtn.com/news/2023-04-25/China-deepens-copyright-cooperation-with-WIPO-1jioyVOxUDS/index.html.
[432] China revises Counter-Espionage Law, News.cn (Beijing) 26 April 2023. Access date: 29 June 2023. https://english.news.cn/20230426/188903dafabf43ad89c90b02aa10a896/c.html.
[433] Chinese FM holds talks with Dutch deputy PM, News.cn (Beijing) 23 May 2023. Access date: 29 June 2023. https://english.news.cn/20230524/403ab082f78a4213924de2f96ae3133e/c.html.
[434] China plans more measures to improve business environment, News.cn (Beijing) 2 June 2023. Access date: 29 June 2023. http://english.news.cn/20230602/789560f93bc1403d9f396338b55dee96/c.html.

Analyst: Irina Popova

France: 0

France has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 19 June 2023, France and South Africa entered an agreement on cyber crime prevention.[435] The partnership provides establishment if an anti-corruption academy in South Africa as to "improve the Special Investigating Unit's cyber forensic capabilities".

France has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

Thus, France receives a score of 0.

Analyst: Nikita Shilikov

Germany: +1

Germany has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 9 December 2022, the Federal Ministry of Justice and the German Patent and Trade Mark Office chaired the meeting on cooperation on intellectual property (intellectual property) rights attended by the heads of offices from the G7 countries and the Director General of the World Intellectual Property Organization.[436] The IP offices of G7 economies agreed to intensify their cooperation on fighting counterfeiting and product piracy. The heads of offices stressed that an "effective response" to these global phenomena would be required. Besides, they agreed to enhance international cooperation as a whole in order to promote a "positive IP culture."

On 21 April 2023, the Federal Office for Information Security (BSI) announced it would offer certification of information technology (IT) products according to the latest standards to make a contribution to increasing the level of cyber security. The new version of the standard defines relevant requirements in more detail. The BSI expressly recommends that manufacturers of IT products use the new standard in order to be prepared not only for technical aspects of domestic regulation but also for the future European certification scheme.[437]

Germany has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows. Germany took strong actions corresponding with privacy and data protection; security; and intellectual property rights both through domestic measures and international cooperation.

Thus, Germany receives a score of +1.

Analyst: Andrey Shelepov

India: +1

India has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 17 November 2022, India and Australia convened their fifth Bilateral Cyber Policy Dialogue in New Delhi. The dialogue was co-chaired by Joint Secretary (Cyber Diplomacy Division) Muanpuii Saiawi from

[435] SA, France sign anti-cyber crime agreement, SA News (Pretoria) 19 June 2023. Access Date: 23 August 2023. https://www.sanews.gov.za/south-africa/sa-france-sign-anti-cyber-crime-agreement

[436] Fight against product piracy: G7 IP leaders intend to intensify cooperation, German Patent and Trade Mark Office (Munich) 9 December 2022. Access Date: 27 April 2023. https://www.dpma.de/english/services/public_relations/press_releases/09122022/index.html.

[437] BSI offers certification according to the latest Common Criteria test standard, German Federal Office for Information Security (Bonn) 21 April 2023. Translation provided by the analyst. Access Date: 27 April 2023. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2023/230421_CC-Standard.html.

Ministry of External Affairs and Dr. Tobias Feakin, Ambassador for Cyber Affairs and Critical Technology, Department of Foreign Affairs and Trade, Government of Australia.[438] The Cyber Policy Dialogue was held under the auspices of the India-Australia Framework Arrangement on Cyber and Cyber-Enabled Critical Technology Cooperation and Plan of Action 2020-2025 for a comprehensive and deeper cyber cooperation.

On 18 November 2022, India presented its Digital Personal Data Protection Bill.[439] The purpose of this Act is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes, and for matters connected therewith or incidental thereto.

On 7 February 2023, the Quad partners of Australia, India, Japan, and the United States are launching a public campaign to improve cyber security across our nations: the Quad Cyber Challenge.[440] The Challenge provides resources, such as basic cybersecurity information and training, for all users – from corporations to education institutions, small businesses, and individuals from grade school students to the elderly. The Quad partners are working to ensure everyone has access to the resources needed to make informed decisions while online and using smart devices.

On 21 February 2023, the Eurasian Patent Organization (EAPO), an international intergovernmental organization of the Eurasian Patent Convention, Moscow and the Council of Scientific and Industrial Research entered into a cooperation on the Traditional Knowledge Digital Library (TKDL).[441] Access through a Non-Disclosure Agreement. Through this Agreement, the EAPO shall gain access to the contents of the TKDL database for the purpose of search and examination of prior art related to Indian traditional knowledge in patent applications, for the purposes of the Intellectual Property Rights (IPR) grant. With this cooperation with EAPO, the number of patent offices worldwide that have access to the TKDL database rises to sixteen.

On 26 May 2023, India announced that it would build a cybersecurity center in Papua New Guinea.[442]

On 29 May - 9 June 2023, the EU Delegation to India facilitated a two-week CBRN-E risk management course for 16 Indian cybersecurity experts in Slovakia.[443] The initiative was organised by the EU-backed project, Enhancing Security Cooperation In and With Asia (ESIWA), which supports deeper security engagement between the EU, its Member States, and ESIWA's partner nations across the Indo-Pacific.

India took strong actions corresponding with privacy and data protection; security; and intellectual property rights both through domestic measures and international cooperation.

Thus, India receives a score of +1.

Analyst: Irina Popova

[438] Fifth India-Australia Cyber Policy Dialogue, Australian Government (Canberra) 17 November 2022. Access Date: 11 April 2023. https://www.internationalcybertech.gov.au/Fifth-India-Australia-Cyber-Policy-Dialogue.
[439] The Digital Personal Data Protection Bill, 2022, Government of India (New Delhi) 18 November 2022. Access Date: 11 April 2023. https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf.
[440] Quad Joint Statement on Cooperation to Promote Responsible Cyber Habits, the White House (Washington DC) 7 February 2023. Access Date: 11 April 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/02/07/quad-joint-statement-on-cooperation-to-promote-responsible-cyber-habits/.
[441] Cooperation between the Eurasian Patent Organization (EAPO), Moscow and the Council of Scientific and Industrial Research (CSIR) on Access to the Traditional Knowledge Digital Library (TKDL), a prior art database of Indian traditional knowledge, Press Information Bureau of Indian Government (New Delhi) 21 February 2023. Access Date: 11 April 2023. https://pib.gov.in/PressReleasePage.aspx?PRID=1901145.
[442] India to build cybersecurity hub in PNG, Post-Courier (Port Moresby) 26 May 2023. Access date: 29 June 2023. https://www.postcourier.com.pg/india-to-build-cyber-security-hub1/.
[443] EU-India enhance security cooperation with CBRN training, Delegation of the European Union to India and Bhutan 8 June 2023. Access date: 29 June 2023. https://www.eeas.europa.eu/delegations/india/eu-india-enhance-security-cooperation-cbrn-training_en?s=167.

Indonesia: +1

Indonesia has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 7-8 December 2022, Indonesia organized the Indonesia Cyber Security Summit – an annual event for all stakeholders in the area of digital security.[444] During the event participants shared an outlook on challenges and solutions towards effective participation against potential cyber threats.

On 2 January 2023, the Government announced a new Criminal Code which would take effect in 2026.[445] The new code contains provisions strengthening the punishment related to trademark and branding infringement, false claim of intellectual property ownership, disclosure of trade secrets.

On 9 February 2023, the National Cyber and Crypto Agency and the Ministry of Education, Culture, Research and Technology agreed to collaborate on promoting Education Computer Security Incident Response Team program aimed to improve human resources capacities in the sphere of digital security.[446]

On 9 March 2023, the National Cyber and Crypto Agency signed a memorandum of understanding with the National Security Authority of Slovakia on increasing cooperation in the sector of cyber security.[447] Both parties emphasized several areas of implementation to be carried out in the next 5 years, namely related to building capacity of human resources in the field of technology.

On 13-14 March 2023, the National Cyber and Crypto Agency held a workshop on risk management and cyber security in the industrial sector.[448] The activity was said to be carried out to assist Electronic System Operators (PSE) in implementing good cybersecurity risk management.

On 14 March 2023, the National Cyber and Crypto Agency held a technical forum on the implementation of vital information infrastructure protection mechanisms.[449] The Agency stressed the importance of maintaining and developing information security system. The participants of the forum shared their knowledge and practice on modern security mechanism to ensure digital information security and digital information security incidents handling.

On 27 March 2023, the National Cyber and Crypto Agency and the Korea International Cooperation Agency officially signed the Record of Discussion "Capacity Development Project for Fostering Cyber

[444] BSSN Invites Indonesian Cybersecurity Stakeholders to Discuss Issues, Trends, and Solutions to Various Challenges of Cybersecurity in the Indonesia Cyber Security Summit 2022 Yogyakarta, National Cyber and Crypto Agency of Indonesia (Jakarta) 7 December 2022. Translation provided by Google Translate. Access Date: 30 April 2023. https://bssn.go.id/bssn-ajak-pemangku-kepentingan-keamanan-siber-indonesia-diskusikan-isu-tren-serta-solusi-berbagai-tantangan-keamanan-siber-dalam-gelaran-indonesia-cyber-security-summit-2022-yogyakarta/

[445] Indonesian New Criminal Code, Baker McKenzie 17 January 2023. Access Date: 30 April 2023. https://globallitigationnews.bakermckenzie.com/2023/01/17/indonesian-new-criminal-code/

[446] BSSN and the Ministry of Education and Culture Agreed on Collaboration, Education Computer Security Incident Response Team Becomes a Featured Program, National Cyber and Crypto Agency of Indonesia (Jakarta) 13 February 2023. Translation provided by Google Translate. Access Date: 30 April 2023. https://bssn.go.id/bssn-dan-kemendikbud-sepakati-kerja-sama-education-computer-security-incident-response-team-jadi-program-unggulan/

[447] Signing Cybersecurity Cooperation, Indonesia Strengthens Relations with Slovakia, National Cyber and Crypto Agency of Indonesia (Jakarta) 16 March 2023. Translation provided by Google Translate. Access Date: 30 April 2023. https://bssn.go.id/tanda-tangani-kerja-sama-keamanan-siber-indonesia-memperkokoh-hubungan-dengan-slowakia/

[448] BSSN Holds Workshop on Risk Management and Cyber Security Maturity in the Industrial Sector, National Cyber and Crypto Agency of Indonesia (Jakarta) 15 March 2023. Translation provided by Google Translate. Access Date: 30 April 2023. https://bssn.go.id/bssn-adakan-workshop-manajemen-risiko-dan-cyber-security-maturity-sektor-industri/

[449] BSSN Invites Ministries/Institutions to Prepare the Acceleration of SPBE Implementation in the Vital Information Infrastructure Sector, National Cyber and Crypto Agency of Indonesia (Jakrata) 15 March 2023. Translation provided by Google Translate. Access Date: 30 April 2023. https://bssn.go.id/bssn-ajak-kementerian-lembaga-siapkan-percepatan-penyelenggaraan-spbe-pada-sektor-infrastruktur-informasi-vital/

Security Professionals (Capacity Development) Project for Nurturing Cybersecurity Professionals) in Indonesia" to provide relevant education and to boost the expertise of human resources.[450]

On 10 April 2023, the National Cyber and Crypto Agency signed a memorandum of understanding and Cooperation Agreement with the Association of Indonesian Internet Service Providers and Indonesian Internet Domain Name Managers to combine efforts to strengthen national cyberspace protection.[451]

On 23 May 2023, the National Cyber and Crypto Agency signed memorandum of understanding (MoU) with Thales, one of the leading private cybersecurity company in the European market.[452] Hinsa Siburian, the Head of the agency mentioned that the MoU signing is in line with the directive of the National Cyber Security Strategy (SKSN), which emphasizes strengthening collaboration with private cyber security companies. The cooperation will develop along three main courses: 1) cyber security services, including risk assessment, training and simulation, as well as detection and response to cyber-attacks; 2) encryption devices and sensors to safeguard crucial information systems; 3) data security platforms, identity and access management as a service, and broader cloud protection.

On 15 June 2023, it was reported that Indonesia's highest cybersecurity body National Cyber and Crypto Agency signed MoU on cyber security cooperation with Huawei as a part of mutual commitment to support cyber security knowledge sharing, thus increasing technological capacities and personnel training in order to further develop cyber resilience of Indonesia.[453]

Indonesia has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows. Indonesia has taken significant steps to improve privacy and data protection, digital security and intellectual property rights.

Thus, Indonesia receives a score of +1.

Analyst: Pavel Doronin

Italy: +1

Italy has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 20-25 November 2022, the National Cybersecurity Agency delegation visited Canada to strengthen bilateral cooperation in the field of cybersecurity.[454] The visit was organized as part of the Agency's international cooperation activities of the Implementation Plan of the National Cybersecurity Strategy 2022-2026. The agenda featured high-level meetings, including a visit to the Canadian Centre for Cyber Security and the University of Ottawa where the National Cybersecurity Agency Director-General Roberto Baldoni gave a lecture on cyber risk management. The National Cybersecurity Agency delegation also participated in the Italian-Canadian Forum on Artificial Intelligence organized by the Italian Chamber of Commerce and contributed to the discussion concerning cybersecurity skills and certification issues.

On 27 November 2022, the National Cybersecurity Agency took part in delivering a capacity-building course on fighting cybercrime for the representatives of national police of nine members of the Association

[450] Implementation of Indonesian and Korean Cooperation, BSSN-KOICA Sign Record of Discussion, National Cyber and Crypto Agency of Indonesia (Jakarta) 27 March 2023. Translation provided by Google Translate. Access Date: 30 April 2023. Kembangkan Kapasitas dan Kapabilitas Keamanan Siber Indonesia, https://bssn.go.id/implementasi-kerja-sama-indonesia-dan-korea-bssn-koica-teken-record-of-discussion-kembangkan-kapasitas-dan-kapabilitas-keamanan-siber-indonesia/

[451] BSSN Signs Collaboration with APJII and PANDI to Strengthen National Cyber Security, National Cyber and Crypto Agency of Indonesia (Jakarta) 10 April 2023. Translation provided by Google Translate. Access Date: 30 April 2023. https://bssn.go.id/bssn-tanda-tangani-kerja-sama-dengan-apjii-dan-pandi-untuk-memperkuat-ketahanan-siber-nasional/

[452] BSSN Holds High-Level Meeting with Thales Indonesia, National Cyber and Crypto Agency of Indonesia 23 May 2023. Translation provided by Google Translate. Access Date: 21 June 2023. https://bssn.go.id/bssn-gelar-high-level-meeting-bersama-thales-indonesia/

[453] Huawei, BSSN Forge Closer Cooperation for Bigger Contribution in Indonesia Cyber Security Development, Antara News 15 June 2023. Access Date: 23 June 2023. https://en.antaranews.com/news/285165/huawei-bssn-forge-closer-cooperation-for-bigger-contribution-in-indonesia-cyber-security-development

[454] Canada: National Cybersecurity Agency on a visit, National Cybersecurity Agency (Rome) 26 November 2022. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/notizie/contenuti/canada-delegazione-acn-missione

of Southeast Asian Nations – Brunei, Cambodia, Indonesia, Laos, Malaysia, the Philippines, Singapore, Thailand, and Vietnam.[455] The course was jointly developed by the Italian Police, the Ministry of Foreign Affairs and International Cooperation, and the National Cybersecurity Agency. Representatives of the Agency highlighted Italy's approach to ensuring cybersecurity and cyber resilience, and presented key elements of the National Cybersecurity Strategy 2022-2026 which aims to increase the cyber capacities of the public administration and reinforce the protection of national infrastructure while ensuring continuous monitoring of cybersecurity risks and analysis of threats, vulnerabilities and attacks.

On 12 December 2022, Director General of the National Cybersecurity Agency Roberto Baldoni and Director General of the Bank of Italy Luigi Federico Signorini signed a memorandum of understanding on the exchange of information and collaboration in the field of cybersecurity.[456] In particular, the Agency and the Bank of Italy will exchange information suitable for preventing and countering cyber incidents and related to attack techniques, tactics and procedures or technologies for prevention of and protection from cyber threats.

On 17 December 2022, Director General Baldoni held the first high-level meeting with Director of North Atlantic Treaty Organization's Cooperative Cyber Defense Centre of Excellence Mart Noorma.[457] The meeting allowed to establish official dialogue between the two institutions and lay the groundwork for developing future synergies and collaborations with the centre. The areas of cooperation which were on the agenda are interinstitutional coordination in the field of data protection and resilience, education, training and research in the information security field, and public-private partnership.

On 9 January 2023, Director General Baldoni met with Microsoft President Brad Smith to discuss collaboration between the two organizations with a view to enhance information security in public and private companies and foster skills and knowledge in the field of cyber risk management.[458] In particular, the National Cybersecurity Agency officially joined the Microsoft Government Security Program which helps government authorities improve cybersecurity.

On 11 January 2023, Director General Baldoni and Secretary General of the Italian Chamber of Deputies Fabrizio Castaldi signed a Memorandum of Understanding (MoU) on cooperation in cyber threat protection.[459] The MoU stipulates various initiatives to enhance capacity-building and training so as to promote skills necessary for managing cyber risks and to proliferate responsible digital culture. The National Cybersecurity Agency will also implement projects aimed at ensuring the required level of information security at the Italian Chamber of Deputies with funds deriving from the National Plan for Recovery and Resilience.

On 12 January 2023, the National Cybersecurity Agency published a new taxonomy to facilitate cyber incident notifications and further impact assessment.[460] The taxonomy makes it mandatory to notify incidents affecting information of networks, systems and services that is not directly conferred under the National Cybersecurity Perimeter, which means that every attempt to access information assets other than those protected within the Perimeter must be reported to the Computer Security Incident Response Team of the National Cybersecurity Agency. The taxonomy stipulates that the notification process concerns all other information assets of the

[455] Cybercrime: National Cybersecurity Agency trains Asian policemen, National Cybersecurity Agency (Rome) 27 November 2022. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/notizie/contenuti/cybercrime-acn-forma-i-poliziotti-asiatici

[456] Agency and Bank of Italy sign a memorandum, National Cybersecurity Agency (Rome) 12 December 2022. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/CS-ACN-BDI.pdf

[457] National Cybersecurity Agency meets NATO Cyber Defense Center Director, National Cybersecurity Agency (Rome) 7 December 2022. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/notizie/contenuti/acn-incontra-il-direttore-del-nato-cyber-defence-centre

[458] Microsoft President visits Agency's headquarters, National Cybersecurity Agency (Rome) 9 January 2022. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/notizie/contenuti/il-presidente-di-microsoft-nel-quartier-generale-di-acn

[459] Agreement between the Chamber of Deputies and the National Cybersecurity Agency on cooperation in cyber threat protection, National Cybersecurity Agency (Rome) 11 January 2023. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/documents/Com.congiuntoCameraACN.pdf

[460] National Cyber Security Perimeter gets reinforced, National Cybersecurity Agency (Rome) 12 January 2023. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/documents/CS_Agenzia_Cybersicurezza_obbligo_notifiche.pdf

Perimeter subjects and must be completed within 72 hours from the moment of detection. The taxonomy is organized in the form of a table, with computer incidents and various phases of an attack classified by categories, and provides an identification code and its corresponding category for each type of cyber incidents. There are six categories of incidents ranging from data exfiltration to targeted phishing and encompassing most information attack techniques described by the international reference for cyber-attack techniques, tactics and procedures.

On 19 January 2023, the National Cybersecurity Agency launched an open call inviting Italian business incubators and accelerators focusing on start-ups in the field of information security and innovation to submit applications for collaboration.[461] After the selection, the Agency will sign cooperation agreements with chosen operators to develop joint programs or adapt those already in place to support participating start-ups with funding. Start-ups will be able to get financial contributions from both the Agency itself and its partners. This initiative comes as part of the strategic program provided for by the National Cybersecurity Strategy 2022-2026 and aimed to support Italian companies and researchers through the establishment of a partnerships network "Cyber Innovation Network." The Agency will thus support the development of new entrepreneurial projects in the field of cybersecurity.

On 20 January 2023, Director General Baldoni and CEO of Cisco Italia Gianmatteo Manghi signed a memorandum of understanding on collaboration for preventing cyber-attacks, supporting cyber resilience and developing digital security of the country through information exchange in the field of subject threat intelligence.[462]

On 23 January 2023, the Training Camp of Cybersecurity National Lab started its work in the city of Turin.[463] This event is supported by the National Cybersecurity Agency and serves as a series of preparation activities ahead of the Italian Cybersecurity Olympiad. At the Camp, 360 high school students benefit from extensive training offered by cybersecurity professionals in such fields as threat intelligence and risk management. The program is part of the Implementation Plan of the National Cybersecurity Strategy 2022-2026.

On 25 January 2023, Director General Baldoni and Co-President of Computer Emergency Response Team of the Italian Financial sector (CERTF) Pierfrancesco Gaggi signed a MoU on the information security of the Italian financial sector.[464] The document is aimed at strengthening the public-private capacity to prevent and respond to threats and cyber-attacks. In order to deal more effectively with cyber risks, the Agency and CERTF in have decided to enhance the institutional dialogue and sharing of data, surveys and statistical analysis on the status and evolution of cybersecurity and data protection, including through promotion of awareness of users and companies on the issues of digital safety, implementation of dedicated communication campaigns and exercises and simulations aimed at enhancing the ability to prevent and react to information incidents.

On 26 January 2023, the National Cybersecurity Agency completed the evaluation of 76 projects submitted by 35 regional and local administrations to invest in strengthening systems of information protection of citizens' private data and public data in Italian regions, metropolitan cities and autonomous provinces.[465]

[461] Agency supports the development of Italian cyber businesses, National Cybersecurity Agency (Rome) 19 January 2023. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/comunicato_ecosistema_startup20230119.pdf

[462] Agency and Cisco sign a memorandum of understanding, National Cybersecurity Agency (Rome) 20 January 2023. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/notizie/contenuti/siglato-protocollo-d-intesa-tra-acn-e-cisco

[463] Agency participates in the Training Camp of Cybersecurity National Lab, National Cybersecurity Agency (Rome) 24 January 2023. Translation provided by the analyst. Access Date: 11 March 2023. https://www.acn.gov.it/notizie/contenuti/acn-partecipa-ai-training-camp-del-cybersecurity-national-lab

[464] Agency and CERTFin sign an agreement on cybersecurity of the financial sector, National Cybersecurity Agency (Rome) 26 January 2023. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/documents/Comunicato%20stampa%20Protocollo%20CERTFin_ACN.pdf

[465] National Plan for Recovery and Resilience: Agency publishes its final ranking of projects for strengthening cyber-resilience of local public administrations, National Cybersecurity Agency (Rome) 26 January 2023. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/notizie/contenuti/pnrr-pubblicata-la-graduatoria-finale-dell-avviso-per-il-potenziamento-della-resilienza-cyber-delle-pa-locali

The Agency admitted 51 projects to receive funding worth EUR45 million from the National Plan for Recovery and Resilience. The projects are to be completed by November 2024.

On 7 February 2023, the National Cybersecurity Agency joined the EU Safer Internet Day with launching the Italian campaign entitled "Together for a better Internet."[466] The initiative is designed to raise people's awareness of privacy and sensitive data protection risks that one can face online and to promote responsible and cautious use of the Internet. The campaign features a number of easy-to-implement solutions and tips to protect one's accounts, adopt secure passwords and control online activities of children with regards to games they play, apps they use and sites they visit.

On 13 February 2023, Director General Baldoni signed a cooperation agreement with the IMT (Institutions, Markets, Technologies) High School of Lucca laying the foundation for joint national and international research programs and projects and other functional initiatives for the promotion and dissemination of the culture of information security.[467]

On 28 February 2023, the National Cybersecurity Agency co-sponsored an initiative by Google "Google.org Impact Challenge: Tech for Social Good."[468] The project is aimed at supporting non-profit organizations, academic and research institutions, as well as Italian social enterprises working on projects focused on creating a safer digital society. Selected Italian organizations will benefit from up to EUR3 million and 6 months of technical guidance to help develop their information security projects. Selected organizations will also have the opportunity to join the technological development support program provided for by the National Cybersecurity Strategy 2022-2026, primarily on such issues as ensuring data security and privacy.

On 3 March 2023, the National Cybersecurity Agency published a Measure Implementation Manual which complements the National Cybersecurity Strategy 2022-2026.[469] The manual contains metrics and measurement indicators for the calculation of Strategy-related key performance indicators and allows to verify the level of effectiveness of cybersecurity investments, research and development activities and awareness building. The set of 261 indicators comprising 82 measures were adopted as a result of collaboration between the Agency and twenty other governmental bodies identified as stakeholders responsible for the implementation of individual cybersecurity measures.

On 26 April 2023, the National Cybersecurity Agency and the National Police signed a MoU to enhance collaboration in the areas of regulation and planning for safeguarding national cybersecurity.[470] The MoU stipulates further information exchange between the two institutions to enable timely coordination to prevent security threats and protect all subjects involved, within the institutions' respective areas of operation. For its inspection tasks, the Agency will be able to use the capacities of the Postal Police Service, such as the Operational Centers for Cybersecurity of the Postal Police, to activate operational support during its security interventions. Finally, the MoU provides for collaboration in planning and implementation of highly specialized training courses in the field of cybersecurity.

[466] Nine recommendations on Safer Internet Day, National Cybersecurity Agency (Rome) 7 February 2023. Translation provided by the analyst. Access Date: 12 March 2023. https://www.acn.gov.it/notizie/contenuti/nove-consigli-per-l-internet-safer-day

[467] Cyber risk management, the lectio magistralis of Prof. Baldoni, National Cybersecurity Agency (Rome) 13 February 2023. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/notizie/contenuti/gestione-del-rischio-cyber-la-lectio-magistralis-del-prof-baldoni

[468] Agency co-sponsors a Google initiative on cybersecurity, National Cybersecurity Agency (Rome) 28 February 2023. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/notizie/contenuti/acn-patrocina-l-iniziativa-google-org-per-la-cybersicurezza

[469] National Cybersecurity Strategy: manual with measurement indicators is published online, National Cybersecurity Agency (Rome) 3 March 2023. Translation provided by the analyst. Access Date: 10 March 2023. https://www.acn.gov.it/notizie/contenuti/strategia-nazionale-di-cybersicurezza-online-il-manuale-con-gli-indicatori-di-misurazione

[470] Cooperation agreement with the State Police to prevent and manage cyber threats (Rome) 26 April 2023. Translation provided by the analyst. Access Date: 01 May 2023. https://www.acn.gov.it/notizie/contenuti/accordo-di-collaborazione-con-la-polizia-di-stato-per-prevenire-e-gestire-gli-eventi-cibernetici

On 1 June 2023, the National Cybersecurity Agency became the national coordinator for the European Cybersecurity Month which is the main EU project on cybersecurity awareness.[471] The initiative, promoted at European level since 2013, provides for the cooperation of the EU Member States, the European Commission, and the European Union Agency for Cybersecurity on the coordinated implementation of annual campaigns aimed at increasing awareness of the risks arising from the use of information technologies and the dissemination of good practices. As part of its mandate, the Agency will deal with the identification and evaluation of awareness initiatives implemented by the private sector and public authorities.

On 16 June 2023, the National Cybersecurity Agency has launched a procedure that allows candidates to submit their expression of interest to collaborate with the Agency, which will help form a team of skilled experts composed of 50 units that will officially part of the Agency's structure.[472] The pool of experts will be created in implementation of the law establishing the National Cybersecurity Agency which identifies the following thematic profiles: technological transformation processes, digital transformation projects, including the development of digital programs and platforms with large-scale dissemination, communication and dissemination activities. The procedure will enable the Agency to establish a pool of resources suitable for these professional profiles.

On 22 June 2023, the National Cybersecurity Agency published the Research and Innovation Agenda for Cybersecurity 2023-2026.[473] The document was developed in partnership with the Ministry of Universities and Research. It aims to stimulate investments in research and innovation in the field of cybersecurity to enhance the protection of the country and reinforce its strategic autonomy. There are six interdisciplinary areas covered by the Agenda: data security and privacy, management of cyberthreats, security of software and digital platforms, security of digital infrastructure, and aspects of engaging the society and government.

On June 23 2023, the National Cybersecurity Agency signed a cooperation agreement with the Conference of Rectors of Italian Universities (CRUI) aimed at promoting academic and professional training on the issues of cybersecurity, as well as joint participation in national and international research projects and the organization of initiatives useful for the promotion and dissemination of the culture of cybersecurity, both in academia and more generally in society.[474] With regard to academic training, CRUI will therefore carry out coordination activities aimed at supporting universities in interacting with the Agency and in defining best practices to face the challenge of skill shortage in cybersecurity. In addition, CRUI and the Agency will jointly act as coordinating bodies for professional training initiatives for public and private parties on the issues of information security. Both Parties are also committed to participating in national and international programs and research projects. Finally, the agreement facilitates the exchange of information and good practices between all the actors involved, including the academia, companies, public entities, and research institutions, and provides for organizing conferences, debates, seminars, and other initiatives functional to the promotion and dissemination of the culture of cybersecurity.

On 6 July 2023, the President of the Council of Ministers adopted a directive titled "Coordination and organization guidelines aimed at promoting the adequate and coordinated management of cyber threats, incidents and crisis situations of a cybernetic nature."[475] The document strengthens the framework for

[471] Agency is the ECSM national coordinator for Italy, National Cybersecurity Agency (Rome) 1 June 2023. Translation provided by the analyst. Access Date: 28 June 2023. https://www.acn.gov.it/notizie/contenuti/acn-e-coordinatore-nazionale-per-litalia-delleuropean-cybersecurity-month

[472] The procedure for the creation of a pool of experts is underway, National Cybersecurity Agency (Rome) 16 June 2023. Translation provided by the analyst. Access Date: 15 August 2023. https://www.acn.gov.it/notizie/contenuti/al-via-la-procedura-per-la-creazione-di-un-contingente-di-esperti

[473] Italy embraces the challenge of emerging technologies, National Cybersecurity Agency (Rome) 22 June 2023. Translation provided by the analyst. Access Date: 28 June 2023. https://www.acn.gov.it/notizie/contenuti/l-italia-raccoglie-la-sfida-delle-tecnologie-emergenti

[474] Agency and CRUI sign a cooperation agreement, National Cybersecurity Agency (Rome) 23 June 2023. Translation provided by the analyst. Access Date: 28 June 2023. https://www.acn.gov.it/notizie/contenuti/firmato-l-accordo-di-collaborazione-tra-acn-e-crui

[475] Strengthening the coordinated response to cyber crises is essential to protect the country, National Cybersecurity Agency (Rome) 7 August 2023. Translation provided by the analyst. Access Date: 15 August 2023. https://www.acn.gov.it/notizie/contenuti/rafforzare-la-risposta-coordinata-alle-crisi-cibernetiche-e-essenziale-per-tutelare-il-paese

cooperation between the public administration and the National Cybersecurity Agency to ensure the ample collaboration with the Agency by public institutions impacted by cyber threats and incidents. It also aims to reinforce the country's cyber resilience, reduce the risks of possible propagation of harmful cyber-attack consequences, or of the recurrence of similar attacks against public and private entities.

On 8 August 2023, the National Cybersecurity Agency published the Guidelines for the creation of IT emergency response teams dedicated to the detection, analysis and response to IT security incidents, as well as to prevention and mitigation of cyber risks.[476] The Guidelines, prepared in accordance with the standards, best practices and frameworks established at the national and international level are an operational tool to support public authorities who wish to enhance their information security.

Italy has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows. Italy took strong measures corresponding with privacy and data protection and information security and supported them with robust international action.

Thus, Italy receives a score of +1.

Analyst: Vadim Kuznetsov

Japan: +1

Japan has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 24 November 2022, Japan announced a plan to create a new organization to develop and maintain country's capacities against cyberattacks.[477]

On 7 December 2022, Japan and the United Kingdom decided to establish a partnership in the field of digital collaboration.[478] The Partnership is aimed to support already existing bilateral agreements while creating new infrastructure for mutual digital development. The key pillars of the Partnership are claimed to be digital infrastructure and technologies, data privacy and protection, digital regulations and standards, digital transformation.

On 8-9 December 2022, the National Center of Incident Readiness and Strategy for Cybersecurity hosted the International Cybersecurity Workshop, Exercise and Tour.[479] During the workshop participants discussed the means of critical infrastructure protection and public-private partnerships in each country.

On 16 December 2022, the Government approved a Cabinet decision on security-related strategic documents: the National Security Strategy (NSS), the National Defense Strategy, and Defense Buildup Program.[480] The NSS contains provisions relating to national cyber defense and marks the restructuration of the National Center for Incident Readiness and Strategy for Cybersecurity to establish a new cybersecurity organization, which will coordinate policies in the field of cybersecurity and will command the cyber units of the Japan Self-Defense Force and the police.

[476] The Guidelines for the realization of CSIRT are available, National Cybersecurity Agency (Rome) 8 August 2023. Translation provided by the analyst. Access Date: 15 August 2023. https://www.acn.gov.it/notizie/contenuti/disponibili-le-linee-guida-per-la-realizzazione-di-csirt

[477] Japan considers creating new defense body for fighting cyberattacks, Japan Times 24 November 2022. Access Date: 30 April 2023. https://www.japantimes.co.jp/news/2022/11/24/national/cyberattacks-organization-security/

[478] UK-Japan Digital Partnership, the Government of UK 7 December 2022. Access Date: 30 April 2023. https://www.gov.uk/government/publications/uk-japan-digital-partnership/uk-japan-digital-partnership

[479] The Result of "International Cybersecurity Workshop, Exercise and Tour 2022", National Center for Incident Readiness and Strategy for Cybersecurity (Tokyo) 15 December 2022. Access Date: 30 April 2023. https://www.nisc.go.jp/eng/pdf/Intl_WS_exercise_tour(EN).pdf

[480] National Security Strategy of Japan, Cabinet Secretariat of Japan (Tokyo)16 December 2022. Access Date: 30 April 2023. https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf

On 17 January 2023, the Ministry of Economy, Trade and Industry held the 9th Meeting of the Japan-China Joint Intellectual Property Working Group online.[481] During the meeting, the parties discussed and exchanged relevant practices for improving the protection of intellectual property rights.

On 7 February 2023, the Quad Cybersecurity Partnership released a joint statement on Cooperation to Promote Responsible Cyber Habits.[482] The joint statement marked the launch of a public campaign to improve cyber security across Australia, India, Japan, and the United States: the Quad Cyber Challenge. The Challenge offers resources, such as basic cybersecurity information and training, for all users from corporations to education institutions, small businesses, and individuals from grade school students to the elderly.

On 10 March 2023, the Ministry of Economy, Trade and Industry reported that the Cabinet of Japan approved draft amendments to intellectual property laws.[483] The main contents of the amendment are following: 1) Extension of trademarks that can be protected; 2) Measures to prevent imitation of product forms in the digital space; 3) Enhanced protection of trade secrets and shared data with limited access; 4) Electronic submission of documents; 5) Strengthening of penalties for bribery of foreign public officials.

On 25 April 2023, the Cabinet approved the Bill for Partial Revision of the Unfair Competition Prevention Act amending Japan's Unfair Competition Prevention Act and other intellectual property (IP) laws.[484] The key amendments introduced were: 1) improving IP protection due to business diversification and digitalization by broadening types of registered trademarks, bolstering protection against data leakage; 2) developing better mechanisms for online submission of applications for IP rights; 3) imposing stricter penalties for bribery and international trade secret infringement.

On 10 June 2023, the Government planned to shift its policy regarding artificial intelligence from promoting to restricting.[485] The concerns were based on copyright infringement linked to generated artificial intelligence technology. Prime Minister Fumio Kishida stated that several amendments to IP law were being examined by the government.

On 19 June 2023, it was announced that the Japan-Association of Southeast Asian Nations (ASEAN) Cybersecurity Capacity Building Centre held the first training session of the ASEAN-Japan Capacity Building Program Enhancement Project on Security and Digital Trust Services.[486] The session was attended by a total of 14 participants from ASEAN countries.

On 23 June 2023, the Government announced that it would require contractors to meet U.S. cybersecurity guidelines to protect sensitive information.[487] The national cybersecurity body mentioned that the changes will take effect during fiscal year 2023/24.

[481] Japanese and Chinese Government Organizations Held Exchange of Views Toward Stronger Protection of Intellectual Property Rights, Ministry of Economy, Trade and Industry of Japan (Tokyo) 19 January 2023. Access Date: 30 April 2023. https://www.meti.go.jp/english/press/2023/0119_001.html

[482] Quad Joint Statement on Cooperation to Promote Responsible Cyber Habits, National Center for Incident Readiness and Strategy for Cybersecurity (Tokyo) 7 February 2023. Access Date: 30 April 2023. https://www.nisc.go.jp/eng/pdf/Quad_Joint_Statement_on_Cooperation_to_Promote_Responsible_Cyber_Habits.pdf

[483] Cabinet Decision on the Bill for Partial Revision of the Unfair Competition Prevention Act, etc., Ministry of Economy, Trade and Industry of Japan (Tokyo) 10 March 2023. Translation provided by Google Translate. Access Date: 30 April 2023. https://www.meti.go.jp/press/2022/03/20230310002/20230310002.html

[484] Revisions to Japanese Unfair Competition Prevention Act and IP Laws to Take Effect June 2023, Lexology 25 April 2023. Access Date: 22 June 2023. https://www.lexology.com/library/detail.aspx?g=5bf2c33d-6b4a-4b55-ae05-c09a80e2bbfe

[485] Intellectual Property Plan Signals Reversal on AI Policy, The Japan News 10 June 2023. Access Date: 22 June 2023. https://japannews.yomiuri.co.jp/politics/politics-government/20230610-115423/

[486] ASEAN-Japan Cybersecurity Capacity Building Center (AJCCBC) Opening Ceremony for 1st Training: Contributing to Developing Cybersecurity Professionals in ASEAN Countries, Japan International Cooperation Agency 19 June 2023. Translation provided by Google Translate. Access Date: 22 June 2023. https://www.jica.go.jp/information/press/2023/20230619_42.html

[487] Japan to require government contractors meet U.S. cybersecurity rules, Nikkei 23 June 2023. Access Date: 23 June 2023. https://asia.nikkei.com/Politics/Defense/Japan-to-require-government-contractors-meet-U.S.-cybersecurity-rules

Japan has taken significant steps to improve privacy and data protection, digital security and intellectual property rights.

Thus, Japan receives a score of +1.

Analyst: Pavel Doronin

Korea: 0

Korea has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 28 November 2022, Korea and the European Union announced the launch of the Korea-EU Digital Partnership.[488] The parties agreed to increase practical cooperation in cybersecurity by means of enhancing sharing in expertise and information on emerging cyberthreats. Also, the parties agreed to jointly promote capacity building in other partner countries.

On 14 December 2022, the Ministry of Science and ICT (MSIT) presented the Fifth Science and Technology Master Plan till 2027.[489] According to the presented plan, Korea would increase investment in emerging technologies including artificial intelligence and foster public-private military cooperation in order to provide better security of the national sovereignty in cyberspace. Cybersecurity was also presented as a distinct sphere of cooperation among other key technological domains.

On 2 January 2023, the MSIT announced the allocation of KRW1.4308 trillion (USD1.08 billion) for research and development (R&D) activities in the ICT sphere for 2023.[490] The MSIT aims at providing better opportunities for developments in artificial intelligence and semiconductors by means of securing top-tier talents and growth of world-class researchers and scholars. The ministry would seek opportunities to provide "the explosive diffusion of research achievements."

On 20 February 2023, the MSIT presented the K-Network 2030 Strategy. The document embraces issues related to nation-wide network development including stability and safety.[491] As to improve network experience, the MSIT claims to promote implementation of modern standards including Wi-Fi 7, upgrade the system capacity of submarine cables, and diversify the cable landing stations.

Korea has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows. Korea has taken strong actions in order to provide better cybersecurity, and at least one action was of international nature.

Thus, Korea receives a score of 0.

Analyst: Alexander Ignatov

[488] Korea and the EU Launch the ROK – EU Digital Partnership, Ministry of Science and ICT (Sejong-si) 28 November 2022. Access Date: 4 May 2023.
https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=759&formMode=&pageIndex=&searchCtgry1=&searchCtgry2=&searchCtgry3=&RLS_YN=&searchOpt=ALL&searchTxt=
[489] The Fifth Science and Technology Master Plan (2023 – 2027) Announced, Ministry of Science and ICT (Sejong-si) 14 December 2022. Access Date: 4 May 2023.
https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=762&formMode=&pageIndex=&searchCtgry1=&searchCtgry2=&searchCtgry3=&RLS_YN=&searchOpt=ALL&searchTxt=
[490] MSIT Confirms Comprehensive Implementation Plan for 2023 R&D Project, Ministry of Science and ICT (Sejong-si) 2 January 2023. Access Date: 4 May 2023.
https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=766&formMode=&pageIndex=&searchCtgry1=&searchCtgry2=&searchCtgry3=&RLS_YN=&searchOpt=ALL&searchTxt=
[491] MSIT Launches the K-Network 2030 Strategy, Ministry of Science and ICT (Sejong-si) 20 February 2023. Access Date: 4 May 2023.
https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=783&formMode=&pageIndex=&searchCtgry1=&searchCtgry2=&searchCtgry3=&RLS_YN=&searchOpt=ALL&searchTxt=#wrap

Mexico: 0

Mexico has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 30 January 2023, the Government installed the Inter-Ministerial Commission for Information and Communication Technologies and Information Security (CITICSI).[492] The CITICSI I is a transversal coordination mechanism, focused on technology management and information security. The Commission aims to act as a coordination instance between authorities, participate in the implementation of strategies and actions for the use of information and communication technologies, and information security, and promote the development of relevant activities.

On 8 February 2023, members of the Parliamentary Group of the Social Encounter Party proposed a draft decree amending the Federal Law on the Protection of Personal Data Held by Individuals and adding an article to the General Law on the Protection of Personal Data Held by Obligated Subjects.[493] The initiative seeks to define and regulate, in current legislation, the protection of biometric data. The initiative aims to create databases for the exclusive use of those who collect only with express consent and without being able to allow consultation or share the use of the databases to a third party, even if there is the consent of the owner. In addition, it aims to guarantee the confidentiality of said database and the exclusive use of it only by the obligated subject.

On 16 March 2023, Deputy Javier López Casarín submitted for the consideration the initiative that reforms the article 21 of the Constitution of Mexico, proposing to amend the Constitution with the section, defining the concepts of 'cybersecurity' and 'cybercrime'.[494]

On 12 April 2023, the National Guard of Mexico, through the General Scientific Directorate, organized the 2023 Cybersecurity Conference, "Secure Internet for Everyone," which, through virtual conferences with the participation of experts from the three levels of Government, private sector, and civil society, disseminates the importance of responsible use of new information technologies.[495]

On 25 April 2023, Deputy Casarín presented a draft decree for the creation of a Federal Cybersecurity Law in Mexico, which would seek to strengthen the protection of data and information online, implement cybersecurity policies and procedures, create a National Cybersecurity Agency and a National Registry of Cybersecurity Incidents, as well as define offenses and sanctions to combat cyber risks.[496] The new law seeks to address some of the challenges currently facing security in cyberspace in Mexico, such as the lack of definition of crimes, as well as establishing attributions, powers and responsibilities between authorities, and addressing the existence of disaggregated legal instruments and not homogeneous.

Mexico has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows. Mexico took steps in order to provide better cybersecurity. No actions referring to other pillars of the commitment have been found so far.

Thus, Mexico receives the score of 0.

Analyst: Ksenia Dorokhina

[492] Instalada la Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información, Gobierno de México (Mexico City) 30 January 2023. Access Date: 17 June 2023. https://www.gob.mx/citicsi/prensa/instalada-la-comision-intersecretarial-de-tecnologias-de-la-informacion-y-comunicacion-y-de-la-seguridad-de-la-informacion

[493] Gaceta del Senado, Miércoles 08 de febrero de 2023 / LXV/2SPO-82-3164/132106, Sobre el Senado (Mexico City) 8 February 2023.. Access Date: 17 June 2023. https://www.senado.gob.mx/65/gaceta_del_senado/documento/132106

[494] Gaceta Parlamentaria, año XXVI, número 6236-II, jueves 16 de marzo de 2023, Gaceta Parlamentaria (Mexico City) 16 March 2023. Access Date : 17 June 2023. http://gaceta.diputados.gob.mx/Gaceta/65/2023/mar/20230316-II.html#Iniciativa9

[495] National Guard inaugurates Cybersecurity Day 2023 safe internet for all, Seguridad (Mexico) 12 April 2023. Translation provided by Google Translate. Access Date: 4 July 2023. https://seguridad.sspc.gob.mx/contenido/2465/guardia-nacional-inaugura-jornada-de-ciberseguridad-2023-internet-seguro-para-todas-y-todos

[496] Gaceta Parlamentaria Palacio Legislativo de San Lázaro (Mexico City) 25 April 2023. Access Date: 17 June 2023. https://www.diputados.gob.mx/LeyesBiblio/iniclave/65/CD-LXV-II-2P-292/02_iniciativa_292_25abr23.pdf

Russia: 0

Russia has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 25 January 2023, the Ministry of Digital Development, Communications and Mass Media and the Federal Security Service jointly announced the establishment of National Center of Digital Cryptography.[497] The Center is said to start operating in 2024. The goal of the new institution is proliferation of effective cryptographic methods and their practical implementation. Also, the Center aims to facilitate necessary skills development.

On 5 May 2023, the Ministry of Digital Development, Communications and Mass Media presented the Concept of Digital Protection for Children.[498] The aim is to provide better protection for children against cyberthreats by means of necessary skills and competences promotion. The Ministry suggests amendments to school curriculum, launch of secured online resources for adults and younger generations, and organizing special courses for parents on how to protect children online.

Russia has partially taken a action in order to provide better cybersecurity. However, in other spheres of the commitment no substantial action was found.

Thus, Russia receives a score of 0.

Analyst: Alexander Ignatov

Saudi Arabia: +1

Saudi Arabia has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 5 December 2022, the National Cybersecurity Authority (NCA) in cooperation with the Ministry of Education would launch a specialized training program to qualify men and women teachers in cybersecurity and child protection on the Internet.[499]

On 17 December 2022, the Intellectual Property Authority published a set of decisions issued by the intellectual property committees.[500] The publication is aimed to raise awareness of intellectual property and promote a culture of respect for it, together with raising the level of competence of researchers and academics in the fields of intellectual property by reviewing the decisions issued by the committees.

On 22 December 2022, Prince Mohammed bin Salman bin Abdulaziz Al Saud launched the National Intellectual Property Strategy.[501] The strategy is aimed to create a comprehensive intellectual property ecosystem by introducing intellectual property that stimulates innovation and creativity competitiveness.

On 27 December 2022, the NCA announced that it would conduct more than 7,000 cybersecurity assessments for the national entities by 2023.[502] The NCA developed a plan to conduct the cyber assessments for the

[497] The Ministry of ICT to Establish the Digital Cryptography Center, Ministry of Digital Development, Communications and Mass Media (Moscow) 25 January 2023. Translation provided by the analyst. Access Date: 4 May 2023. https://digital.gov.ru/ru/events/42403/

[498] Ministry to Develop Concept of Digital Protection for Children, Ministry of Digital Development, Communications and Mass Media (Moscow) 5 May 2023. Translation provided by the analyst. Access Date: 04 July 2023. https://digital.gov.ru/ru/events/44157/

[499] Saudi Arabia's NCA launches training program to qualify teachers in cybersecurity, Security Middle East 12 December 2022. Access Date: 30 April 2023. https://www.securitymiddleeastmag.com/saudi-arabias-nca-launches-training-program-to-qualify-teachers-in-cybersecurity/

[500]Publication of the decisions of the committees for the settlement of intellectual property disputes), Saudi Authority for Intellectual Property (Riyadh) 17 December 2022. Translation provided by Google Translate. Access Date: 30 April 2023. https://www.saip.gov.sa/en/news/1466/

[501] HRH Crown Prince Launches National Intellectual Property Strategy, Saudi Press Agency (Riyadh) 12 December 2022. Access Date: 30 April 2023. https://www.spa.gov.sa/viewfullstory.php?lang=en&newsid=2411825#2411825

[502] NCA to conduct more than 7,000 cybersecurity assessments for national entities, Saudi Gazette (Riyadh) 27 December 2022. Access Date: 30 April 2023. https://saudigazette.com.sa/article/628385/SAUDI-ARABIA/NCA-to-conduct-more-than-7000-cybersecurity-assessments-for-national-entities

national entities during 2023 in order to monitor the cyber risks at the national level and to measure the commitment level of the entities with the requirements and regulations issued by the authority.

On 13 February 2023, the Saudi Data & AI Authority (SDAIA) launched the Capacity Development Program for Government Entities 2.0 in order to develop national cadres in data management and governance as well as personal data protection.[503] The program aims to support government entities in qualifying specialists to acquire professional certificates in these fields by conducting intensive courses to enrich their skills.

On 27 March 2023, the Council of Ministers approved a series of changes to the Kingdom's Personal Data Protection Law (PDPL) that was issued in 2021.[504] The amended law introduces new concepts and mechanisms that will enhance Saudi Arabia's capabilities to integrate into international data protection standards, such as the EU General Data Protection Regulation. The PDPL's amendments are related to the following: 1) Data transfer mechanisms – International transfers are permitted if they are in implementation of obligations under international agreements to which Saudi Arabia is a party, if it serves national interests, if they are in implementation of any obligations to which the data subject is a party; 2) Basis for data processing – Controllers may now rely on "legitimate interests" as a lawful basis to process and disclose personal data, although this does not apply to sensitive personal data, or processing that contravenes with the rights granted under the PDPL and its executive regulations; 3) Criminal prosecution - Criminal sanctions for violating the PDPL's data transfer restrictions were removed. Only a single instance of criminal offence remains in relation to the disclosure or publication of sensitive personal data in violation of the law. In other cases, the penalties for breaching the PDPL will be a warning or a fine of up to SAR5 million (USD1.3 million) that may be doubled for repeated violations; 4) Registration requirement - The amended law no longer concerns the creation of an electronic portal or any requirement that the controller must register his data processing activities. However, the SDAIA is empowered to issue data protection requirements in cooperation with any other relevant authorities. SDAIA also has the mandate to license auditors and accreditation bodies and establish a national registry if it decides that this would be an appropriate tool and mechanism to monitor auditor compliance.

On 6 April 2023, the Saudi Data & AI Authority signed a memorandum of understanding (MoU) with the Islamic University of Madinah.[505] Under the MoU both parties will make effort to enhance cooperation between the two sectors, achieve government integration, and reinforce adherence to cyber security standards to ensure the safety of the digital technological environment.

On 10 April 2023, the NCA announced that it would host the Global Cybersecurity Forum in Riyadh on 8-9 November 2023.[506]

On 7 June 2023, King Salman issued a decree to establish a new institute for the Global Cybersecurity Forum (GCF) in Riyadh.[507] The institute will be designed to resolve the most challenging issues connected with cybersecurity and data protection of the government, private sector and population. As an international discussion and collaboration platform the institute will help to exchange knowledge and expertise for multinational stakeholders.

[503] SADAIA launches the National Capacity Development Program for government agencies for the year 2023 Saudi Data & AI Authority (Riyadh)13 February 2023. Translation provided by Google Translate. Access Date: 30 April 2023. https://sdaia.gov.sa/ar/MediaCenter/News/Pages/NewsDetails.aspx?NewsID=152#

[504] Amended Saudi Personal Data Protection Law to be in force from September, Saudi Gazette (Riyadh) 10 April 2023. Access Date: 30 April 2023. https://saudigazette.com.sa/article/631462/SAUDI-ARABIA/Amended-Saudi-Personal-Data-Protection-Law-to-come-into-force-in-September

[505] The Islamic University signs a memorandum of understanding with (SDAIA) to build a safe digital technology environment and enable digital transformation at the university), Saudi Data & AI Authority (Riyadh) 6 April 2023. Translation provided by Google Translate. Access Date: 30 April 2023. https://sdaia.gov.sa/ar/MediaCenter/News/Pages/NewsDetails.aspx?NewsID=156

[506] Under Patronage of Custodian of the Two Holy Mosques, NCA to Hold Next Global Cybersecurity Forum in November 2023, Saudi Press Agency 10 April 2023. Access Date: 30 April 2023. https://www.spa.gov.sa/viewfullstory.php?lang=en&newsid=2442664

[507] Saudi Arabia to establish institute for Global Cybersecurity Forum, Arab News 07 June 2023. Access Date: 23 June 2023. https://www.arabnews.com/node/2317396/saudi-arabia

On 8 June 2023, the National Cybersecurity Authority informed that during May 2023 it provided cybersecurity training for more than 400 employees from governmental agencies.[508] The training program is aimed to foster human capacities for preventing and tackling cyber threats. The program consisted of six main courses: governance, risk management and compliance, protection and defense, threat management, vulnerability assessment, response to cyber incidents.

Saudi Arabia has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows. Saudi Arabia has taken significant steps to improve privacy and data protection, digital security and intellectual property rights.

Thus, Saudi Arabia receives a score of +1.

Analyst: Pavel Doronin

South Africa: 0

South Africa partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 19 June 2023, South Africa and France entered an agreement on cyber crime prevention.[509] The partnership provides establishment if an anti-corruption academy in South Africa as to "improve the Special Investigating Unit's cyber forensic capabilities".

On 11 July 2023, the Council for Scientific and Industrial Research in cooperation with Take Note IT (private entity) launched the Cyber Excellence Academy.[510] The Academy aims to provide the locals with advanced skills and knowledge "to combat evolving digital threats". The program's participants would be equipped with the leading expertise delivered by the industry's key players.

South Africa has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows. During the compliance period South Africa has taken actions referring to the cybersecurity component of the commitment.

Thus, South Africa receives a score of 0.

Analyst: Alexander Ignatov

Türkiye: +1

Türkiye has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 30 November 2022, the Presidency's Digital Transformation Office in cooperation with the Presidency of Defense Industries of the Republic of Türkiye held the opening of the Cyber Security Week, aimed to boost the development of the domestic cyber security ecosystem, and increase cyber security awareness and collaborations.[511]

On 20 December 2022, the Presidency's Digital Transformation Office signed the Digital Innovation Cooperation Platform protocol with Türkiye's eight leading universities.[512] The President of the Presidency

[508] The National Academy of Cybersecurity: More than 400 trainees in the "Cyber Pro" program during the month of May, National Cybersecurity Authority of Saudi Arabia 08 June 2023. Translation provided by Google Translate. Access Date: 23 June 2023.

[509] SA, France sign anti-cyber crime agreement, SA News (Pretoria) 19 June 2023. Access Date: 23 August 2023. https://www.sanews.gov.za/south-africa/sa-france-sign-anti-cyber-crime-agreement

[510] Cyber Excellence Academy Launched in collaboration with CSIR, SA News (Pretoria) 11 July 2023. Access Date: 23 August 2023. https://www.sanews.gov.za/south-africa/cyber-excellence-academy-launched-collaboration-csir

[511] Opening Program of Cyber Security Week Held, Presidency's Digital Transformation Office (Ankara) 30 November 2022. Translation provided by Google Translate. Access Date: 30 April 2023. https://cbddo.gov.tr/haberler/6540/siber-guvenlik-haftasi-nin-acilis-programi-gerceklesti-

[512] Digital Innovation Cooperation Platform (DIIB) Protocol Signed, Presidency's Digital Transformation (Ankara) Office 20 December 2022. Translation provided by Google Translate. Access Date: 30 April 2023. https://cbddo.gov.tr/haberler/6553/dijital-inovasyon-is-birligi-platformu-diib-protokolu-imzalandi

Digital Transformation Office, Dr. Ali Taha Koç noted that the platform was aimed to strengthen cooperation between the public and private sectors, as well as academia in the fields of artificial intelligence, data science, cyber security, robotics and related technologies. The cooperation within the framework of the platform will include development of domestic solutions in the area of digital technologies, implementation of short-/long-term training programs in order to foster advanced digital skills of human resources in the public and private sector.

On 9-12 January 2023, the Presidency's Digital Transformation Office organized the Digital State Strategy Focus Group meetings to address the needs identified in different digital segments and to develop solution proposals.[513] The studies were carried out under five main axes: "Strategic Compliance and Governance," "Digital Skills, Data Management in the Public," "Technological Infrastructures," "Service Design and Delivery," "Digital Inclusion and Participation."

On 28 January 2023, the Conference on the Protection of Personal Data in Türkiye was held at Nevşehir Hacı Bektaş Veli University.[514] The aim of the event was declared as overcoming challenges of personal data protection amidst developing technologies.

On 23 March 2023, the Personal Data Protection Authority published an Information Note on Political Parties and Independent Candidates for the Protection of Personal Data in Election Activities stating relevant data protection regulations required for mandatory compliance.[515]

On 1 April 2023, the Information and Communication Technologies Authority Board adopted new regulation regarding data protection of social networks users.[516] From this date social network providers are obliged to keep the data they processed from Türkiye, in Türkiye. In case of non-compliance with the data localization requirement, the Information and Communication Technologies Authority may impose an administrative fine up to 3 percent of the social network providers' global turnover of the previous year.

On 28 April 2023, the European Patent Office and Istanbul Technical University held an award ceremony for the 3rd Universities Patent Competition.[517] The competition was organized with the aim of increasing patent awareness in universities, equipping university students with information they will use in their professional careers and academic studies, encouraging invention activities.

On 1 May 2023, the Turkish Patent and Trademark Office in cooperation with the International Federation of Inventors' Association, the World Intellectual Property Organization and the European Patent Office organized "ISIF Istanbul International Invention Fair."[518]

[513] Digital State Strategy Focus Group Meetings Held, Presidency's Digital Transformation Office (Ankara) 9 January 2023. Translation provided by Google Translate. Access Date: 30 April 2023. https://cbddo.gov.tr/haberler/6591/dijital-devlet-stratejisi-odak-grup-toplantilari-gerceklestirildi

[514] Data Protection Day Event Held in Nevsehir on 28 January, The Personal Data Protection Authority of Türkiye (Ankara) 28 January 2023. Translation provided by Google Translate. Access Date: 30 April 2023. https://www.kvkk.gov.tr/Icerik/7532/28-Ocak-Veri-Koruma-Gunu-Etkinligi-Nevsehir-de-Gerceklestirildi

[515] Public Announcement on Personal Data Processed by Political Parties and Independent Candidates in the Scope of Election Activities, The Personal Data Protection Authority of Türkiye (Ankara) 28 March 2023. Translation provided by Google Translate. Access Date: 30 April 2023. https://kvkk.gov.tr/Icerik/7543/Secim-Faaliyetleri-Kapsaminda-Siyasi-Partiler-ve-Bagimsiz-Adaylar-Tarafindan-Islenen-Kisisel-Veriler-Hakkinda-Kamuoyu-Duyurusu

[516] The Information And Communication Technologies Authority Board's Decision On Procedures And Principles On Social Network Providers Has Been Published, Mondaq 22 June 2023. Access Date: 25 June 2023. https://www.mondaq.com/Türkiye/data-protection/1330480/the-information-and-communication-technologies-authority-boards-decision-on-procedures-and-principles-on-social-network-providers-has-been-published

[517] 'Patent Türkiye 3rd Universities Patent Competition Awards Found Their Owners, Turkish Patent and Trademark Office 28 April 2023. Translation provided by Google Translate. Access Date: 25 June 2023. https://www.turkpatent.gov.tr/haberler/patentle-turkiye-3-universiteler-patent-yarismasi-odul-toreninde-oduller-sahiplerini-buldu

[518] ISIF'23 - Istanbul International Invention Fair, Turkish Patent and Trademark Office 01 May 2023. Access Date: 25 June 2023. https://www.turkpatent.gov.tr/en/news/isif23-istanbul-international-invention-fair

On 21 May 2023, the Presidency Digital Transformation Office and the Council of Higher Education agreed to launch Cyber Security Vocational Schools in four Turkish universities.[519] The aim of these particular schools is to provide qualified workforce to the sector and to create a sustainable workforce development program in vocational schools that will be supported by cooperation models to be developed together with the national cyber security ecosystem. students will be provided with training on subjects such as cyber security incident management, security technology operations, penetration tests, network security, as well as basic courses in the field of cyber security. Subject experts from the industry will also be able to provide specialized trainings in selected field courses.

On 7 June 2023, Head of the Digital Transformation Office Dr. Ali Taha Koç attended the Inaugural Meeting of the OECD Global Forum on Technology in Paris.[520] Speaking at the Beak-Out Session on "Responsible, Values-based and Rights-oriented Technology," underlined the importance of the development of new technologies in an ethical and respectful for human rights-respecting manner and assessment of relevant policy and regulatory framework in order to mitigate emerging risks.

Türkiye has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows. Türkiye has taken significant measures to promote privacy and data protection and to ensure digital security.

Thus, Türkiye receives a score of +1.

Analyst: Pavel Doronin

United Kingdom: 0

The United Kingdom has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 25 November 2022, the United Kingdom and Singapore held the 7th UK-Singapore Financial Dialogue in Singapore.[521] Both countries renewed their commitment to deepening the UK-Singapore Financial Partnership that was agreed in 2021, discussed mutual priorities such as sustainable finance, FinTech and innovation, and agreed on further cooperation in these areas. At the Financial Dialogue, the UK and Singapore agreed on a Memorandum of Understanding on the UK-Singapore FinTech Bridge.

On 30 November 2022, the Government confirmed the Network and Information Systems Regulations would be strengthened to protect essential and digital services against increasingly sophisticated and frequent cyber attacks both then and in the future.[522]

On 7 December 2022, the United Kingdom and Japan decided to establish a partnership in the field of digital collaboration.[523] The Partnership is aimed to support already existing bilateral agreements while creating new infrastructure for mutual digital development. The key pillars of the Partnership are claimed to be digital infrastructure and technologies, data privacy and protection, digital regulations and standards, digital transformation.

On 22 March 2023, the UK-Malaysia Digital Innovation Programme Demo Day kicked off in Sunway City, Kuala Lumpur where 10 UK net zero start-ups pitched their technologies in-person for up to USD1 million

[519] Wanted Personnel of Cyber Security Sector Are Coming, Presidency Digital Transformation Office of Türkiye 21 June 2023. Translation provided by Google Translate. Access date: 25 June 2023. https://cbddo.gov.tr/haberler/6767/siber-guvenlik-sektorunun-aranan-elemanlari-geliyor

[520] The Relationship between Technology and Human Rights was Discussed at the OECD Global Technology Forum, Presidency Digital Transformation Office of Türkiye 07 June 2023. Translation provided by Google Translate. Access date: 25 June 2023. https://cbddo.gov.tr/haberler/6757/oecd-kuresel-teknoloji-forumu-nda-teknoloji-ve-insan-haklari-iliskisi-tartisildi

[521] UK and Singapore deepen collaboration in FinTech and strengthen financial cooperation, The UK Government 25 November 2022 Access Date: 30 March 2023 https://www.gov.uk/government/news/uk-and-singapore-deepen-collaboration-in-fintech-and-strengthen-financial-cooperation

[522] Cyber laws updated to boost UK's resilience against online attacks, The UK Government 30 November 2022 Access Date: 30 March 2023 https://www.gov.uk/government/news/cyber-laws-updated-to-boost-uks-resilience-against-online-attacks

[523] UK-Japan Digital Partnership, the Government of UK 7 December 2022. Access Date: 30 April 2023. https://www.gov.uk/government/publications/uk-japan-digital-partnership/uk-japan-digital-partnership

investment and entry into the Sunway iLabs' Net Zero Lab, an accelerator programme for green start-ups.[524] The initiative also saw UK tech companies connecting and exploring opportunities with the wider tech ecosystem including Malaysia government bodies and venture capital funds. The event was attended by Minister of Economy YB Rafizi Ramli, His Majesty's Trade Commissioner for Asia Pacific Natalie Black, Deputy British High Commissioner David Wallace as well as Sunway Group's Group Chief Executive Officer of Digital and Strategic Investments Evan Cheah.

On 22 March 2023, the United Kingdom published the new Cyber Security Strategy.[525] This would ensure services are better protected from cyber threats, further securing sensitive information and ensuring patients can continue accessing care safely as the National Health Service continues to cut waiting lists.

On 8 June 2023, the UK and the United States have reached a commitment in principle to establish the UK Extension to the Data Privacy Framework, which would see the creation of a new 'data bridge' between the 2 countries.[526] The US companies who are approved to join the framework, would be able to receive UK personal data under the new data bridge. In 2021, the UK exported more than GBP79 million of data-enabled services to the US. A data bridge would speed up processes for businesses, reduce costs, and increase opportunity by making it easier for British business to operate and trade internationally.

On 12 June 2023, Technology Minister Sir John Whittingdale has announced plans to boost digital connectivity across the country, from Wi-Fi in lamp posts and satellites in most rural parts of Scotland.[527] The island of Papa Stour in the Shetland Islands was the first community that gained new digital infrastructure as part of government plans to ensure universal access to fast, reliable broadband coverage.

The United Kingdom has partially complied with the commitment to further enable data free flow with trust and promote cross-border data flows. The United Kingdom has taken actions as to provide better protection against cyberthreats, but no action referring to intellectual property rights enforcement has been found.

Thus, the United Kingdom receives a score of 0.

Analyst: Nikita Shilikov

United States: +1

The United States has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 10 January 2023, the House of Representatives voted in favor of establishing a new select committee on intellectual property rights (IPR) enforcement in competition with China.[528] The committee is ordered to investigate issues related to IPR violations that might be committed by Chinese entities, and make policy recommendations.

[524]UK net zero start-ups keen to tap into Malaysia's tech ecosystem, The UK Government 22 March 2023 Access Date: 30 March 2023 https://www.gov.uk/government/news/uk-net-zero-start-ups-keen-to-tap-into-malaysias-tech-ecosystem
[525] Government sets out strategy to protect NHS from cyber attacks, the UK Government 22 March Access Date: 30 March 2023 https://www.gov.uk/government/news/government-sets-out-strategy-to-protect-nhs-from-cyber-attacks
[526] UK and US reach commitment in principle over 'data bridge', The UK Government 8 June 2023 Access Date: 28 June 2023 https://www.gov.uk/government/news/uk-and-us-reach-commitment-in-principle-over-data-bridge
[527] Bold plans to boost digital connectivity across the country, from wifi in lamp posts and satellites in most rural parts of Scotland, The UK Government 12 June 2023 Access Date: 28 June 2023 https://www.gov.uk/government/news/bold-plans-to-boost-digital-connectivity-across-the-country-from-wi-fi-in-lamp-posts-and-satellites-in-most-rural-parts-of-scotland
[528] New U.S. House Creates Committee Focused on Competing With China, U.S. News (New York) 10 January 2023. Access Date: 4 May 2023. https://www.usnews.com/news/us/articles/2023-01-10/new-u-s-house-creates-committee-focused-on-competing-with-china

On 17 February 2023, the Federal State Commission launched a new office to tackle issues related to data security violating business practices and law enforcement.[529] The Office of Technology is said to boost the Commission's expertise and achieve its mission of "protecting consumers and promoting competition."

On 13 April 2023, the Cybersecurity and Infrastructure Security Agency (CISA) in cooperation with the Federal Bureau of Investigation, the National Security Agency, and the international partners from Australia, Canada, the United Kingdom, Germany, the Netherlands, and New Zealand published the joint guidance "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default."[530] The documents is addressed to software manufacturers to take necessary steps to fulfil the "security-by-design" and the "security-by-default" requirements.

On 14 April 2023, the CISA in partnership with the National Council of Statewide Interoperability Coordinators and the government-led Safety Community (SAFECOM) published the SAFECOM Guidance on Emergency Communications Grants.[531] The guidance assists private entities in receiving funding to invest in emergency communication projects. The guide reflects the current cybersecurity and critical infrastructure landscape, investment priorities, technical standards, etc.

On 19 April 2023, the CISA along with international partners from the United Kingdom, Australia, New Zealand, and Canada published a joint guide on cybersecurity in smart cities.[532] The guide is intended to help communities to went through cybersecurity-related issues during the smart-city integration process. The document contains a list of international best practices on cybersecurity based on principles of secure planning and designing, proactive supply chain risk management, and operational resilience.

The United States has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows. The United States has taken steps matching Pillar 1 of the commitment (promoting privacy and data protection; ensuring security; intellectual property right protection), and at least some of these actions could be considered strong and international by nature.

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

Analyst: Alexander Ignatov

European Union: +1

The European Union has fully complied with the commitment to further enable data free flow with trust and promote cross-border data flows.

On 30 November 2022, the European Data Protection Supervisor and the European Union Agency for Cybersecurity signed a Memorandum of Understanding (MoU) creating strategic cooperation framework. Both entities agreed to jointly cooperate on capacity building and awareness-raising activities. The MoU also includes a strategic plan to promote the awareness of cyber hygiene, privacy and data protection amongst EU institution, bodies and agencies.[533]

On 13 December 2022, the European Commission initiated the process to adopt an adequacy decision for the EU-US Data Privacy Framework to support trans-Atlantic data flows in respect of privacy

[529] FTC Launches New Office of Technology to Bolster Agency's Work, Federal Trade Commission (Washington D.C.) 17 February 2023. Access Date: 4 May 2023. https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-launches-new-office-technology-bolster-agencys-work

[530] U.S. and International Partners Publish Secure-by-Design and -Default Principles and Approaches, Cybersecurity & Infrastructure Security Agency (Washington, D.C.) 13 April 2023. Access Date: 4 May 2023. https://www.cisa.gov/news-events/news/us-and-international-partners-publish-secure-design-and-default-principles-and-approaches

[531] CISA, SAFECOM and NCSWIC Publish SAFECOM Guidance on Emergency Communications Grants, Cybersecurity & Infrastructure Security Agency (Washington, D.C.) 14 April 2023. Access Date: 4 May 2023. https://www.cisa.gov/news-events/news/cisa-safecom-and-ncswic-publish-safecom-guidance-emergency-communications-grants-0

[532] U.S., U.K., Australia, Canada and New Zealand Release Cybersecurity Best Practices for Smart Cities, Cybersecurity & Infrastructure Security Agency (Washington, D.C.) 19 April 2023. Access Date: 4 May 2023. https://www.cisa.gov/news-events/news/us-uk-australia-canada-and-new-zealand-release-cybersecurity-best-practices-smart-cities

[533] Pairing up Cybersecurity and Data Protection Efforts: EDPS and ENISA sign Memorandum of Understanding, European Union Agency for Cybersecurity (Athens) 30 November 2022. Access Date: 30 April 2023. https://www.enisa.europa.eu/news/pairing-up-cybersecurity-and-data-protection-efforts-edps-and-enisa-sign-memorandum-of-understanding

compliance.[534] The Adequacy Decision was drafted following an in-depth review of the US Data Privacy Framework, which concluded that the US provides an adequate level of protection for personal data transferred from the EU to the US.

On 16 January 2023, the EU Network and Information Security Directive 2 entered into force, replacing original NIS Directive, which was introduced in 2016 as the first cybersecurity regulation introduced in EU scale.[535] NIS 2.0 aims to enforce EU cybersecurity capacities and capabilities by involving a larger number of sectors involved and to standardize security requirements. The Directive also mandates the creation of new mechanisms to promote effective cooperation between national authorities and a new entity to superintend coordinated actions in response to full-scale cyber-attacks – the European Cyber Crises Liaison Organisation Network.

On 26 January 2023, the European Union Agency for Cybersecurity organized the EU Cybersecurity Policy Conference with the aim of providing networking opportunities of sharing views and practices to key stakeholders of EU cybersecurity policy.[536]

On 1 February 2023, the EU and Singapore signed Digital Partnership to strengthen cooperation in digital technology area.[537] Digital partnership includes joint research and development cooperation on high-tech projects and ensures trusted cross border data flows in compliance with data protection rules and other public policy objectives.

On 6 February 2023, it the EU and India jointly established a new Trade and Technology Council.[538] It was stated that within the Council, three working groups would be created to organize their work in three different areas including cybersecurity and digital cooperation.

On 7 February 2023, the European Union Agency for Cybersecurity hosted the Cybersecurity Standardization Conference 2023 to hold discussion over standardization activities related to existing and emerging legislation.[539]

On 24 February 2023, the European Data Protection Board adopted three guidelines in the final version: Guidelines on the Interplay between the application of Art. 3 and the provisions on international transfers as per Chapter V of the General Data Protection Regulation, which provides guidelines on certification as a tool for transfers and guidelines on deceptive design patterns in social media platform interfaces.[540]

On 28 February 2023, the EU Legal Affairs Committee introduced a new mechanism to protect local craft and industrial products marked with geographical indication.[541]

On 15 March 2023, the European Data Protection Board launched its 2023 Coordinated Enforcement Action.[542] Within the framework of the activity 26 Data Protection Authorities (DPAs) of the European Economic Area in the nomination and position of Data Protection Officers. The Data Protection Officers

[534] Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision, European Commission (Brussels) 13 December 2022. Access Date: 30 April 2023. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632
[535] The NIS2 Directive: A high common level of cybersecurity in the EU, European Parliament (Brussels) 8 February 2023. Access Date: 30 April 2023. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
[536] EU Cybersecurity Policy Conference, European Union Agency for Cybersecurity (Athens) 26 January 2023. Access Date: 30 April 2023. https://www.enisa.europa.eu/events/enisa-cyber-security-policy-conference-2023
[537] EU and Singapore launch Digital Partnership, European Commission (Brussels) 1 February 2023. Access Date: 30 April 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_467
[538] EU-India: new Trade and Technology Council to lead on digital transformation, green technologies and trade, European Commission (Brussels) 6 February 2023. Access Date: 30 April 2023. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_596
[539] Cybersecurity Standardisation Conference 2023, European Union Agency for Cybersecurity (Athens) 7 February 2023. Access Date: 30 April 2023. https://www.enisa.europa.eu/events/cybersecurity_standardisation_2023/cybersecurity_standardisation_2023
[540] EDPB publishes three guidelines following public consultation, European Data Protection Board (Brussels) 24 February 2023. Access Date: 30 April 2023. https://edpb.europa.eu/news/news/2023/edpb-publishes-three-guidelines-following-public-consultation_en
[541] New EU mechanism to protect local craft and industrial products, European Parliament 28 February 2023. Access Date: 30 April 2023. https://www.europarl.europa.eu/news/en/press-room/20230227IPR76586/new-eu-mechanism-to-protect-local-craft-and-industrial-products
[542] Launch of coordinated enforcemenxt on role of data protection officers, European Data Protection Board 15 March 2023. Access Date: 30 April 2023. https://edpb.europa.eu/news/news/2023/launch-coordinated-enforcement-role-data-protection-officers_en

will serve as intermediaries between DPAs, individual and the business units of an organization. The Officers will foster compliance with data protection law and promotion of data subject rights.

On 30 March 2023, the European Commission proposed to establish a new unit within the EU's Intellectual Property Office to support transparency in standard essential patents licensing.[543]

On 17 April 2023, the European Data Protection Board (EDPB) adopted the final version of the Guidelines on data subject rights - Right of access.[544] The final version contains an extended analysis of various aspects of the right of access and provides definitive guide on right of access implementation. In addition, the EDPB also adopted final versions of the targeted updates of Guidelines for identifying a controller or processor's lead supervisory authority and the Guidelines on data breach notification.

On 18 April 2023, the European Commission adopted proposal for the EU Cyber Solidarity Act to bolster EU's cybersecurity capacities.[545] The Act will improve the detection and awareness mechanisms of cybersecurity threats, support preparedness of critical entities and reinforce crisis management capabilities. The European Commission additionally presented Cybersecurity Skills Academy, as part of the 2023 European Year of Skills in response to existing cybersecurity talent gap.

On 11 May 2023, the European Parliament adopted the EU-U.S. Data Privacy Framework resolution on the adequacy of the protection.[546]

On 25 May 2023, the European Union Agency for Cybersecurity hosted Cybersecurity Certification Conference in order to provide a platform for discussion of the impact of upcoming EU laws and frameworks on cybersecurity certification and consider solutions to challenges brought up by the cybersecurity certification requirements related to new technologies.[547]

On 1 June 2023, the Unified Patent Court (UPC) is coming into force as an entity with an exclusive jurisdiction over Unified Patents in Europe.[548] The UPC will provide uniform protection across all participating countries, thus lowering the costs and reducing administrative burdens associated with litigation for patent holders.

On 6 June 2023, the Council of the EU and the Parliament reached an agreement on the directive concerning financial services contracts concluded at a distance.[549] The Commission proposal repeals the 2002 directive, and introduces new provisions for financial services contracts concluded at a distance as an additional chapter of the consumer rights directive which protect consumers in all kinds of commercial practices. The aim is to provide consumers a higher level of protection when accessing new financial products and services from their phones and computers.

On 26 June 2023, the Council of the EU and the European Parliament reached a provisional agreement on a regulation aimed at ensuring a high common level of cybersecurity across the EU institutions, bodies,

[543] Commission to propose competence centre on essential tech patents, EURACTIV (Brussels) 30 March 2023. Access Date: 30 April 2023. https://www.euractiv.com/section/digital/news/commission-to-propose-competence-centre-on-essential-tech-patents/
[544] EDPB adopts final version of Guidelines on data subject rights - right of access, European Data Protection Board (Brussels) 17 April 2023. Access Date: 30 April 2023. https://edpb.europa.eu/news/news/2023/edpb-adopts-final-version-guidelines-data-subject-rights-right-access_en
[545] Cyber: towards stronger EU capabilities for effective operational cooperation, solidarity and resilience, European Commission 18 April 2023. Access Date: 28 June 2023. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2243
[546] European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework, European Parliament 11 May 2023. Access Date: 28 June 2023. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html
[547] Exploring the Feasibility of EU Cybersecurity Certification in support of New Technologies, European Union Agency for Cybersecurity 25 May 2023. Access Date: 28 June 2023. https://www.enisa.europa.eu/news/exploring-the-feasibility-of-eu-cybersecurity-certification-in-support-of-new-technologies
[548] The unitary patent system, European Commission (Brussels) . Access Date: 30 April 2023. https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/patent-protection-eu/unitary-patent-system_en
[549] Council and Parliament reach provisional political agreement on financial services contracts concluded at a distance, Council of the EU. Access Date: 17 June 2023. https://www.consilium.europa.eu/en/press/press-releases/2023/06/06/council-and-parliament-reach-provisional-political-agreement-on-financial-services-contracts-concluded-at-a-distance/

offices and agencies proposed by the Commission in March 2022.[550] The new regulation will create a common framework for all the EU entities in the field of cybersecurity and will improve their resilience and incident response capacities.

On 28 June 2023, the Data Act which aims to boost the EU's data economy by unlocking industrial data, optimising its accessibility and use, and fostering a competitive and reliable European cloud market.[551] It seeks to ensure that the benefits of the digital revolution are shared by everyone. The Act includes: measures that enable users of connected devices to access the data generated by these devices and by services related to these devices; measures to provide protection from unfair contractual terms that are unilaterally imposed; mechanisms for public sector bodies to access and use data held by the private sector in cases of public emergencies such as floods and wildfires; new rules that grant customers the freedom to switch between various cloud data-processing service providers; measures to promote the development of interoperability standards for data-sharing and data processing, in line with the EU Standardisation Strategy.

On 28 June 2023, the Council of the EU reached an agreement with the European Parliament on the Data Act.[552]

On 4 July, the European Commission proposed a new law to streamline cooperation between DPAs when enforcing the General Data Protection Regulation in cross-border cases.[553] The new regulation will set up concrete procedural rules for the authorities when applying the GDPR in cases which affect individuals located in more than one Member State. The proposal will contribute to reduce disagreements and facilitate consensus among authorities since the initial stages of the process. The new regulation provides detailed rules to support the smooth functioning of the cooperation and consistency mechanism established by the GDPR, harmonising rules in the following areas: rights of complainants, rights of parties under investigation (controllers and processors), streamlining cooperation and dispute resolution etc.

On 10 July 2023, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework.[554] The decision concludes that the United States ensures an adequate level of protection – comparable to that of the European Union – for personal data transferred from the EU to US companies under the new framework. Based on the new adequacy decision, personal data can flow safely from the EU to US companies participating in the Framework, without having to put in place additional data protection safeguards.

On 11 July 2023, the Commission adopted a new strategy on Web 4.0 and virtual worlds to steer the next technological transition.[555] The strategy is in line with the 2030 objectives of the Digital Decade policy programme and three of its key pillars of digitalisation: skills, business and public services. The fourth pillar, infrastructures, is addressed by the Commission's connectivity package and its broader efforts on computing, cloud and edge capacities. It also addresses the openness and global governance of virtual worlds and Web 4.0 as a specific strand of action.

[550] Cybersecurity at the EU institutions, bodies, offices and agencies: Council and Parliament reach provisional agreement, Council of European Union (Brussels) 26 June 2023. Access Date: 18 August 2023. https://www.consilium.europa.eu/en/press/press-releases/2023/06/26/cybersecurity-at-the-eu-institutions-bodies-offices-and-agencies-council-and-parliament-reach-provisional-agreement/

[551] Data Act: Commission welcomes political agreement on rules for a fair and innovative data economy, European Commission (Brussels) 28 June 2023. Access Date: 18 August 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3491

[552] Better access to and use of data: MEPs reach agreement with Council. Access Date: 18 August 2023. https://www.europarl.europa.eu/news/en/press-room/20230626IPR00843/better-access-to-and-use-of-data-meps-reach-agreement-with-council

[553] Data protection: Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases. Access Date: 18 August 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609

[554] Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows, European Commission (Brussels) 10 July 2023. Access Date: 18 August 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

[555] Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds, European Commission (Brussels) 11 July 2023. Access Date: 18 August 2023. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3718

On 19 July, the Council of the EU and the European Parliament reached a common position on the Cyber Resilience Act.[556] The draft regulation introduces mandatory cybersecurity requirements for the design, development, production and making available on the market of hardware and software products to avoid overlapping requirements stemming from different pieces of legislation in EU member states.

The European Union has fully committed to further enable data free flow with trust and promote cross-border data flows. The European Union has taken significant steps to improve privacy and data protection, digital security and intellectual property rights.

Thus, European Union receives a score of +1.

Analyst: Pavel Doronin

[556] Cyber resilience act: member states agree common position on security requirements for digital products, Council of European Union (Brussels) 19 July 2023. Access Date: 18 August 2023. https://www.consilium.europa.eu/en/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/