2022 G20 Bali Summit Interim 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 29 April 2023

July 14, 2023

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

Contents

Preface 3
Research Teams 4
G20 Research Group 4
CIIR G20 Research Team 4
Introduction and Summary 5
Methodology and Scoring System 5
Commitment Breakdown 5
Selection of Commitments 5
Interim Compliance Scores 6
Interim Compliance by Member 6
Interim Compliance by Commitment 6
Table 1: 2022 G20 Bali Summit Commitments Selected for Compliance Monitoring 7
Table 2: 2022 G20 Bali Summit Interim Compliance Scores 8
Table 3: 2022 G20 Bali Summit Interim Compliance by Member 9
Table 4: 2022 G20 Bali Summit Interim Compliance by Commitment 10
Table 5: G20 Compliance by Member, 2008-2021 11
Conclusions 13
Further Research and Reports 13
Considerations and Limitations 13
Appendix: General Considerations 14
1. Macroeconomics: Price Stability 15
2. Macroeconomics: Fiscal Resilience 44
3. Trade: Open Agricultural Trade 54
4. Digital Economy: Data Flow with Trust 62
5. Crime and Corruption: Bribery 89
6. Labour and Employment: Gender Equality 145
7. Development: Common Framework for Debt Treatment 172
8. Food and Agriculture: Food Security 189
9. Health: Global Health Governance 213
10. Health: Universal Health Coverage 246
11. Energy: Zero- and Low-Emission Power Generation 275
12. Energy: Energy Access 300
13. Environment: Land Protection 324
14. Environment: Sustainable Development 354
15. Climate: Paris Agreement 383

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		0	
Brazil			+1
Canada		0	
China			+1
France	−1		
Germany			+1
India			+1
Indonesia			+1
Italy			+1
Japan			+1
Korea		0	
Mexico		0	
Russia		0	
Saudi Arabia			+1
South Africa	−1		
Türkiye		0	
United Kingdom		0	
United States			+1
European Union			+1
Average	+0.45 (73%)		

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."[235]

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."[236] 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."[237] 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

[235] 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
[236] 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
[237] 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."[238] 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."[239]

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."[240] 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."[241] The same year the Osaka Track on Data Free Flow with Trust was launched as to facilitate multilateral discussion on related issues.[242]

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."[243] In Riyadh the G20 leaders re-committed to "further facilitate data free flow and strengthen consumer and business trust."[244]

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."[245] 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."[246]

[238] 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
[239] 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
[240] 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
[241] 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
[242] 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
[243] 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
[244] 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
[245] 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
[246] 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."[247]

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."[248]

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."[249]

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.[250] "Personal data" refers to "any information relating to an identified or identifiable individual (data subject).[251]

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;

[247] 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

[248] 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.

[249] 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

[250] 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

[251] 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.[252]

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."[253] 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."[254]

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."[255]

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;

[252] The OECD Privacy Framework, OECD (Paris) 2013. Access Date: 3 February 2023. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[253] 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
[254] 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
[255] 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.[256]

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."[257]

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;

[256] 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
[257] 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.[258] 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.[259]

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

[258] 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.
[259] 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.[260] 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.[261]

On 30 March 2023, the second meeting of the "Data Governance and Privacy Protection" commission of the Federal Council for transparency was held.[262] 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.

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.

Analyst: Irina Popova

Australia: 0

Australia has partly 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 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.[263]

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

[260] 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.

[261] 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.

[262] 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.

[263] 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.

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.[264] That contributes to the Pillar 1 "Ensuring security" component of the commitment by encouraging the use of international standards and best practices on digital security risk management.

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.[265] That contributes to the Pillar 1 "Ensuring security" component of the commitment by supporting the development of a skilled workforce that can manage digital security risk.

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. 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.[266] That contributes to the Pillar 1 "Ensuring security" by encouraging the use of international standards and best practices on digital security risk management.

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.[267]

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. However, no action referring to the Pillar 1 components of enforcing intellectual property rights, and providing better user data protection has been founded. Also, no action taken by Australia could be considered to be international by nature.

Thus, Australia receives a score of 0.

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.[268] 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.

[264] 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
[265] 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
[266] 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
[267] 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/.
[268] 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.

On 16 March 2023, the ANPD hosted the World Bank Digital Development specialist Julian Najles for a technical meeting.[269] 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.[270] 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.[271] 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.[272] 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 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.[273] 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.

[269] 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.

[270] 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.

[271] 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.

[272] 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.

[273] 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.

O 6 April 202, the three 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.[274] 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.

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.[275] 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.[276] 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.

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.[277]

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

[274] 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.

[275] 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

[276] 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/

[277] 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

Internet access to over 36,000 homes in over 350 rural, remote and indigenous communities across the province.[278]

On 23 February 2023, Minister of Public Safety Marco Mendicino, announced new funding for two innovative cybersecurity projects at the Université de Sherbrooke.[279] 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.[280] 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.

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.[281]

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.[282] 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

[278] 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

[279] 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

[280] 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/

[281] 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.

[282] 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.

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.[283] 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.[284] The Administrative Measures primarily consist 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.[285] 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.

China has taken strong actions on data protection and cybersecurity, including through international cooperation.

Thus, China receives a score of +1.

Analyst: Irina Popova

France: −1

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

During the monitoring period, no action was taken by France as to comply with the commitment.

Thus, France receives a score of −1.[286]

Analyst: Nikita Shilikov

[283] 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.

[284] 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.

[285] 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.

[286] This score of non-compliance is awarded after searching on the following websites: Government of France https://www.gouvernement.fr/; Ministry of Economy, Finance and Industrial and Digital Sovereignty of France https://www.economie.gouv.fr/; Ministry for Europe and Foreign Affairs of France https://www.diplomatie.gouv.fr/fr/

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.[287] 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.[288]

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 Ministry of External Affairs and Dr. Tobias Feakin, Ambassador for Cyber Affairs and Critical Technology, Department of Foreign Affairs and Trade, Government of Australia.[289] 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.[290] 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.[291] The Challenge

[287] 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.

[288] 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.

[289] 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.

[290] 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.

[291] 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/.

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).[292] 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.

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

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.[293] 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.[294] 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.[295]

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.[296]

[292] 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.

[293] 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/

[294] 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/

[295] 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/

[296] 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/

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.[297] 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.[298] 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 Security Professionals (Capacity Development) Project for Nurturing Cybersecurity Professionals) in Indonesia" to provide relevant education and to boost the expertise of human resources.[299]

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.[300]

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.[301] 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.

[297] 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/

[298] 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/

[299] 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/

[300] 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/

[301] 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

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 of Southeast Asian Nations – Brunei, Cambodia, Indonesia, Laos, Malaysia, the Philippines, Singapore, Thailand, and Vietnam.[302] 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.[303] 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.[304] 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.[305] 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.[306] 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.[307] 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

[302] 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

[303] 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

[304] 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

[305] 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

[306] 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

[307] 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

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 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.[308] 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.[309]

On 23 January 2023, the Training Camp of Cybersecurity National Lab started its work in the city of Turin.[310] 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.[311] 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.[312]

[308] 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

[309] 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

[310] 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

[311] 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

[312] 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."[313] 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.[314]

On 28 February 2023, the National Cybersecurity Agency co-sponsored an initiative by Google "Google.org Impact Challenge: Tech for Social Good."[315] 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.[316] 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.[317] 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.

Italy took strong measures corresponding with privacy and data protection and information security and supported them with robust international action.

[313] 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
[314] 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
[315] 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
[316] 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
[317] 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

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.[318]

On 7 December 2022, Japan and the United Kingdom decided to establish a partnership in the field of digital collaboration.[319] 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.[320] 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.[321] 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.

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.[322] 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.[323] 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.[324] The main contents of the amendment are

[318] 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/
[319] 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
[320] 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
[321] 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
[322] 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
[323] 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
[324] 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

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.

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 partly 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.[325] 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.[326] 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.[327] 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.[328] 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 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

[325] 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=
[326] 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=
[327] 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=
[328] 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 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.[329]

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 a score of 0.

Analyst: Alexander Ignatov

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.[330] 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.

Russia has taken a strong action in order to provide better cybersecurity.

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.[331]

On 17 December 2022, the Intellectual Property Authority published a set of decisions issued by the intellectual property committees.[332] 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.

[329] 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

[330] 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/

[331] 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/

[332] 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/

On 22 December 2022, Prince Mohammed bin Salman bin Abdulaziz Al Saud launched the National Intellectual Property Strategy.[333] 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.[334] The NCA developed a plan to conduct the cyber assessments for the 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.[335] 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.[336] 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.[337] 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 November 8-9, 2023.[338]

[333] 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

[334] 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

[335] 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#

[336] 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

[337] 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

[338] 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

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: −1

South Africa has failed to comply with the commitment to further enable data free flow with trust and promote cross-border data flows.

During the compliance period no action taken by South Africa and aimed at implementation of the commitment has been found.

Thus, South Africa receives a score of −1.[339]

Analyst: Alexander Ignatov

Türkiye: 0

Türkiye has partially 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.[340]

On 20 December 2022, the Presidency's Digital Transformation Office signed the Digital Innovation Cooperation Platform protocol with Türkiye's eight leading universities.[341] The President of the Presidency 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.[342] 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."

[339] This score of non-compliance is awarded after searching on the following websites: South African Government https://www.gov.za; The Presidency https://www.thepresidency.gov.za/; South African National CSIRT https://www.cybersecurityhub.gov.za/; Department of Communications & Digital Technologies https://www.dcdt.gov.za/; South African Government News Agency https://www.sanews.gov.za/

[340] 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-

[341] 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

[342] 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

On 28 January 2023, the Conference on the Protection of Personal Data in Türkiye was held at Nevşehir Hacı Bektaş Veli University.[343] 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.[344]

Türkiye has taken some efforts to promote privacy and data protection and to ensure digital security.

Thus, Türkiye receives a score of 0.

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.[345] 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.[346]

On 7 December 2022, the United Kingdom and Japan decided to establish a partnership in the field of digital collaboration.[347] 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 investment and entry into the Sunway iLabs' Net Zero Lab, an accelerator programme for green start-ups.[348] 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.

[343] 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

[344] 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

[345] 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

[346] 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

[347] 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

[348] 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

On 22 March 2023, the United Kingdom published the new Cyber Security Strategy.[349] 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.

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.[350] The committee is ordered to investigate issues related to IPR violations that might be committed by Chinese entities, and make policy recommendations.

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.[351] 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."[352] 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.[353] 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.[354] The guide is intended to help communities to went through cybersecurity-related issues during the smart-city integration process.

[349] 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
[350] 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
[351] 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
[352] 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
[353] 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
[354] 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

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 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 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. MoU also includes a strategic plan to promote the awareness of cyber hygiene, privacy and data protection amongst EU institution, bodies and agencies.[355]

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 compliance.[356] 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.[357] 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.[358]

On 1 February 2023, the EU and Singapore signed Digital Partnership to strengthen cooperation in digital technology area.[359] 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.

[355] 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

[356] 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

[357] 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

[358] 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

[359] 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

On 6 February 2023, it the EU and India jointly established a new Trade and Technology Council.[360] 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.[361]

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.[362]

On 28 February 2023, the EU Legal Affairs Committee introduced a new mechanism to protect local craft and industrial products marked with geographical indication.[363]

On 15 March 2023, the European Data Protection Board launched its 2023 Coordinated Enforcement Action.[364] 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 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.[365]

On 17 April 2023, the European Data Protection Board (EDPB) adopted the final version of the Guidelines on data subject rights - Right of access.[366] 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 1 June 2023, the Unified Patent Court is coming into force as an entity with an exclusive jurisdiction over Unified Patents in Europe.[367] It will provide uniform protection across all participating countries, thus lowering the costs and reducing administrative burdens associated with litigation for patent holders.

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

[360] 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
[361] 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
[362] 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
[363] 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
[364] 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
[365] 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/
[366] 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
[367] 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