GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

MAY 20, 2024
(Corrected)

GDA COMMENTS TO DATA PROTECTION AUTHORITY OF TÜRKİYE

DRAFT REGULATION ON THE PROCEDURES AND PRINCIPLES REGARDING THE TRANSFER OF PERSONAL DATA ABROAD

The Global Data Alliance (GDA)[1] welcomes the opportunity to offer comments to the Data Protection Authority of Türkiye on the Public Announcement of the Draft Regulation on the Procedures and Principles Regarding the Transfer of Personal Data Abroad (hereinafter "draft Data Transfer Regulations").[2]

The GDA is a cross-industry coalition of companies, headquartered across the world that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs. The GDA supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade.

GDA member companies are active in many sectors of Türkiye's economy. GDA members collectively support hundreds of thousands of jobs and support numerous activities that advance inclusive growth, innovation, and economic development in Türkiye.

The GDA supports many aspects of Türkiye's Data Transfer Regulations. We particularly recognize and appreciate that the Data Transfer Regulations appear to be designed for interoperability with the EU's General Data Protection Regulation (GDPR) and other cross-border data frameworks around the world. Our comments focus primarily on Article 14 on Standard Contractual Clauses. In this regard, our comments focus on two core issues:

1. Recognizing the benefits of international data transfers.
2. Promoting convergence and interoperability among contractual transfer mechanisms.

Overview of Relevant Provisions

Article 14 of the draft Data Transfer Regulations state as follows:

> **Providing appropriate assurance with a standard contract**

ARTICLE 14- (1) Appropriate assurance can be provided through a standard contract that includes issues such as data categories, purposes of data transfer, recipient and recipient groups, technical and administrative measures to be taken by the data recipient, additional measures taken for sensitive personal data.

(2) The standard contract is determined and announced by the Board.

(3) The standard contract must be used without any modification. If the standard contract is concluded in a foreign language, the Turkish text is taken as basis.

(4) The standard contract is concluded between the parties to the transfer of personal data. The standard contract must be signed by the parties to the transfer or by persons authorized to represent and sign the parties.

(5) The standard contract is notified to the Authority within five working days from the completion of the signatures, either physically or by registered electronic mail (KEP) address or other methods determined by the Board. In the standard contract, the transfer parties can specify who will fulfill the notification obligation. If no determination has been made in this regard, the standard contract is notified to the Authority by the data exporter.

(6) Documents proving that the signatories of the standard contract are authorized and a notarized translation of each document in a foreign language are attached to the notification to be made.

(7) In the event that the standard contract announced by the Board is amended or there is no valid signature of one or both of the transfer parties in the standard contract, an examination is carried out by the Board in accordance with Article 15 of the Law.

Discussion

In this discussion, we focus on two core issues:

1. Recognizing the benefits of international data transfers.
2. Promoting convergence and interoperability among contractual transfer mechanisms.

1. Recognizing the Benefits of International Data Transfers

We welcome the Data Transfer Regulation's recognition of the importance of cross-border data transfers. At a time of rising data protectionism across the world, Türkiye should continue to promote strong privacy safeguards and international data flows as pillars of the data economy. As reflected in the GDA Cross-Border Data Policy Index,[3] there remain a significant number of data localization mandates or data transfer restrictions in Türkiye. It is hoped that the more flexible regime established with the draft Data Transfer Regulations will lead to a trend of relaxation of some of the data localization mandates or data transfer restrictions scattered throughout various sector-specific regulations.

The ability to transfer data securely across transnational digital networks is of central importance to many other national Turkish policy objectives. Data transfers support cybersecurity, fraud prevention, anti-money laundering, and other activities relating to the protection of health, privacy, security, and regulatory compliance.

This ability also supports greater economic prosperity for Türkiye's economy. Data transfers are estimated to contribute $2.8 trillion to global GDP, a share that exceeds the global trade in goods and is expected to grow to $11 trillion by 2025.[4] Furthermore, the ability to transfer data across borders is critical to any economy that wishes to realize the benefits of digital transformation and artificial intelligence (AI). AI is expected to add the $13 trillion dollars to global GDP by 2030.[5]

Conversely, those economies that restrict their own ability to access and share data across transnational digital networks are less likely to benefit from these beneficial economic shifts. According to studies by the World Trade Organization, United Nations, and Organisation for Economic Cooperation and Development (OECD), cross-border data restrictions harm GDP (minus 0.7-1.7%); investment flows (minus 4%); and small business (up to 80% higher trade costs).[6] As stated by the World Bank,

> Restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies and especially on trade in services. Studies show that countries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies, whereas the benefits of reducing data restrictions on trade in services would on average be about 5 percent.[7]

In sum, unnecessary restrictions on data transfers have broad reverberations that can lead to reduced GDP, foreign investment, and job growth for the countries that adopt these restrictions, as well as adverse impacts on local and national digital ecosystems – at a time when economic recovery is top of agenda for every government.

The ability to transfer data across borders is also critical to Turkish companies of all sizes and across all industry sectors, as well as workers, consumers, and other citizens. Turkish companies that do business internationally need to send data across national borders every day, including to:

- Access marketplaces, purchasers, suppliers, and other commercial partners in other countries;
- Contribute to product innovation, research and development (R&D), and product improvement activities taking place in multiple jurisdictions, and ensure operational consistency and efficiency (e.g., in human resources);
- Monitor product reliability and safety for consumers or users;
- Ensure legal and regulatory compliance; and
- Support supply chain resilience and visibility;
- Maintain visibility and rapid response capability vis-à-vis cybersecurity threats in different countries in real-time.[8]

For Turkish companies, transferring data across borders helps them be more efficient and effective at delivering the products and services their customers demand. Data transfers also underpin global products and services that support virtual collaboration, online training, and online education, among many others. Having access to these global tools is particularly important for small- and medium-sized enterprises, which often leverage them to reach new markets and service new customers.[9] Finally, cross-border transfers are also integral to international supply chains, which must move information across borders to optimize sourcing, finance, logistics, risk mitigation, and responsiveness.[10]

With a view to safeguarding these various priorities while advancing high standards of data protection, we urge Türkiye to follow the so-called "accountability principle," which is the prevailing international global norm that governs the relationship between personal data protection and cross-border data transfers. Under this norm, organizations that transfer data globally should implement procedures to ensure that data will continue to be protected, even if it is transferred to countries other than where it was first collected. The accountability principle was first developed by the OECD,[11] and was subsequently endorsed and has been integrated in many legal systems including the EU,[12] Japan,[13] New Zealand,[14] Singapore,[15] and Canada.[16] This principle is also a significant feature of the APEC Privacy Framework,[17] the APEC Privacy Recognition for Processors (PRP) system,[18] the APEC Cross Border Privacy Rules (CBPR) system,[19] and the ASEAN Model Contractual Clauses.[20]

2. Promoting convergence and interoperability among contractual transfer mechanisms

To leverage the benefits that are brought about by responsible flow of data across borders, we recommend Türkiye promote convergence and interoperability of data transfer mechanisms. We commend the inclusion of data transfer mechanisms that have become a key instrument for both protecting data subjects' rights and for the development of the digital economy and international trade. We encourage you to prioritize transfer mechanisms that are based on high levels of data protection, trust, and confidence.

We welcome the Draft Data Transfer Regulation's reference to multiple transfer mechanisms, which can help ensure companies have multiple ways to transfer data, consistent with their business models and appropriate safeguards. For example, we note that the Bill, the Draft Data Transfer Regulations are based on,references to adequacy determinations, as well as standard contractual clauses and binding corporate rules. Different types of organizations and different business models require the use of different transfer mechanisms that are not interchangeable. In practice, larger companies will often rely on one or more data transfer mechanisms, using the tool most tailored to their business needs and to the specific data transfer(s) at hand. Other companies may principally rely only on one mechanism, such as adequacy determinations or standard contractual clauses. Creating a range of flexible transfer mechanisms that can be used differently in these different situations will help companies transfer data responsibly, consistent with Turkish law.

We observe, however, that Draft Data Transfer Regulations do not currently contain a detailed discussion of other transfer mechanisms, such as certification mechanisms, codes of conduct, or other international instruments and agreements. We would recommend that references to these three mechanisms – at a minimum for purposes of future development – be included.

Data transfer mechanisms designed for use by companies operating in one country also cannot be viewed in isolation from mechanisms created and used in other countries. As countries worldwide develop and update their personal information protection laws and regulations it is critical that these legal frameworks are designed to effectively protect privacy in a manner that is internationally interoperable, flexible enough to account for rapid evolution in both technologies and business models, levels of risk, and that prioritizes high standards of data protection. This is particularly important in the context of international data transfers, where interoperable legal requirements support organizations' ability to comply with obligations across jurisdictions.

Of course, the context and perspective around privacy and personal data protection may appropriately vary among different countries based on cultural expectations, legal traditions, and other factors. At the same time,

governments should support the common recognition of international norms and practices around core substantive protections that underpin interoperable privacy frameworks. If countries instead adopt fragmented policies on core issues it raises the cost of business for all companies and can undermine personal data protection and consumer privacy.

As Türkiye looks to finalize and implement the Regulations, we recommend that it recognize that existing contractual transfer mechanisms may provide contractual safeguards consistent with Türkiye's legal requirements and therefore satisfy Article 14, so long as those contracts contain sufficiently similar substantive protections. Many global companies have already adopted contract-based transfer mechanisms that protect data as it is transferred between countries and regions. We encourage Türkiye to recognize that these existing contracts may already satisfy Article 14 – without requiring companies to re-negotiate those contracts to adopt specific pre-approved language or formats. This approach to contractual transfer safeguards drives harmonization by recognizing alignment between these existing mechanisms and Turkish legal requirements – and ensures that companies can leverage existing compliance practices and mechanisms in support of products, services, and customers in Türkiye.[21] In addition, participation in international certification systems can also advance convergence and interoperability.

GDA member companies have adopted contractual transfer mechanisms including the:

- European Union's Standard Contractual Clauses (EU SCCs);
- United Kingdom's International Data Transfer Agreements (UK IDTAs); and
- The Global Cross Border Privacy Rules System and the accompanying Privacy Rules for Processors

We also **recommend that Türkiye prioritize flexibility in the appropriate format for standard contractual arrangements**, including for existing contractual arrangements that already meet substantive obligations of Turkish law. For example, one interoperable approach that Türkiye could consider to leveraging existing contractual mechanisms is to create a model addendum that can be added onto other contractual mechanisms, such as an addendum to the EU SCCs. The UK Information Commissioner's Office (UK ICO) recently adopted this approach in two new sets of model contractual clauses that came into force this year.[22] The creation of such addenda – which recognize the substantive protections in the underlying contractual transfer mechanism and adopt a set of additional protections designed to satisfy the requirements of a second jurisdiction – helps support interoperability of data transfer mechanisms across jurisdictions.[23]

Finally, if Türkiye adopts new model SCCs under Article 14, **we encourage Türkiye to account for the range of different entities that transfer data and the range of different transfers between these entities.** Any new contractual mechanism should support transfers between two controllers, from a controller to a processor, from a processor to a controller, or between processors.[24] Data transfers take many shapes and forms and it is important that contractual transfer mechanisms can be used in the full range of transfer scenarios. For example, the EU recently updated its SCCs to adopt a modular approach that organizations can use to support these different types of transfers. Whether Türkiye adopts a modular approach or not, any new SCCs in Türkiye should be flexible enough to be used in each of these scenarios.

3. Comments on Binding Corporate Rules

We welcome also welcome the additional safeguards on Binding Corporate Rules and the increasing alignment with the EU's General Data Protection Regulations Considering the nature of globalized businesses, our recommendation for sustainable and scalable BCRs would be:

- Eliminate unnecessary administrative tasks and procedures which do not contribute to the effectiveness of data protection such as a requirement to provide contact details of each member of the group to which BCR's apply.
- Requirements for BCR's legally binding instruments (commitments) should be further clarified. Additional clarity is welcome if other instruments than intracompany agreements would be considered as legally binding.
- Introduce a threshold that only "substantive" changes to the BCRs and underlying supporting policies should be notified to the board.
- Introduce a mechanism for recognition and interoperability of the BCRs approved by other Data Protection Authorities in similar fashion UK ICO has approached recognition of EU approved BCRs and SCCs.

4. Procedural Comments

We would appreciate if the Data Protection Authority would consider extending consultation periods to secure effective participation of wide range of stakeholders. Current timelines are challenging to say the least. Many stakeholders have been engaging in this process for several years and have had constructive engagements but the approach seems to continue to evolve and change. It would be useful to have more time to digest the different approaches and have more substantive discussions about why the changes are being pursued and what the specific objectives are.

Conclusion

We appreciate the opportunity to share these views and hope that they will be helpful as Türkiye considers its next steps on the draft Policy. Please do not hesitate to contact us with any questions regarding this submission.

[1] GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. GDA member companies have operations and support millions of jobs across all 50 US states. For more information, see https://www.globaldataalliance.org

[2] *See* https://www.kvkk.gov.tr/Icerik/7906/Kisisel-Verilerin-Yurt-Disina-Aktarilmasina-Iliskin-Usul-ve-Esaslar-Hakkinda-Yonetmelik-Taslagi-Hakkinda-Kamuoyu-Duyurusu

[3] Global Data Alliance, *Cross-Border Data Policy Index* (2024), at: https://globaldataalliance.org/resource/cross-border-data-policy-index/

[4] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, 297 OECD Digital Economy Papers 24 (August 2020).

[5] https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-AI-frontier-modeling-the-impact-of-ai-on-the-world-economy#/

[6] *See* Global Data Alliance, *Cross-Border Data Policy Index, supra* note 3.

[7] *See* The World Bank, *World Development Report* (2020), https://www.worldbank.org/en/publication/wdr2020.

[8] In the healthcare sector specifically, another important priority is to facilitate the transfer of data used in clinical trials, product-safety assessments, provision of technical support to patients or healthcare providers, and monitoring of relevant healthcare applications.

[9] USAID Digital Strategy, 2020–2024, https://www.usaid.gov/usaid-digital-strategy, p. 37 ("Digital ecosystems have the potential to equip informal merchants, women entrepreneurs, smallholder farmers, and MSMEs engaged in cross-border trade with access to markets, information, and finance").

[10] Global Data Alliance, Cross-Border Data Transfers & Supply Chain Management, available at https://www.globaldataalliance.org/downloads/03182021gdaprimersupplychain.pdf.

[11] OECD Privacy Framework 2013 (p15), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[12] Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[13] Act on the Protection of Personal Information, https://www.ppc.go.jp/en/legal/

[14] Privacy Act 2020, https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

[15] Personal Data Protection Act 2012, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[16] Personal Information Protection and Electronic Documents Act fair information principles, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

[17] APEC Privacy Framework, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[18] APEC Privacy Recognition for Processors

[19] APEC Cross Border Privacy Rules system, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

[20] ASEAN Model Contractual Clauses (2021), at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf; *See also,* Singapore Personal Data Protection Commission, Guidance for Use of ASEAN Model Contractual Clauses for Cross-Border Data Flows in Singapore (2022), at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Singapore-Guidance-for-Use-of-ASEAN-MCCs.pdf?la=en#:~:text=The%20ASEAN%20Model%20Contractual%20Clauses%20%28ASEAN%20MCCs%29%20are,parties%20that%20protects%20the%20data%20of%20data%20subjects.

[21] A touchstone of future regulatory efforts should be to seek to ensure interoperability between Turkish regulations and those of the EU, the USA and other jurisdictions. As Türkiye considers the possibility of new regulatory requirements, we encourage the establishment of reasonable grace periods and due respect for business predictability and legal certainty.

[22] *See* UK ICO, International Data Transfer Agreement and Guidance, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. First, the

UK ICO adopted a 36-page standalone set of contract terms that companies could adopt to support transfers of data from the UK. Second, the UK ICO adopted a separate nine-page addendum, which companies can add to existing contracts that incorporate the EU SCCs; this allows companies to adopt the additional language in the addendum to support transfers of data from the UK. Adopting both a standalone set of SCCs and an addendum creates flexible options for companies transferring data from the UK, including for smaller businesses (which may not have other contractual mechanisms in place and thus may not make use of the addendum) and larger ones (which may already have existing contractual mechanisms that are readily modified by the addendum).

[23] We recommend ensuring that companies may seek to adhere by reference to a model addendum. Parties could provide that their contractual agreements incorporate the model addendum by reference, while noting that the agreement may provide for more specific terms on particular issues.

[24] We also note that in complex intercompany relationships, a particular entity may have different roles in different contexts, with respect to different information sets, and at different times, including as a controller, processor, importer, and/or exporter.