THE EU'S NEW DATA FLOW AGREEMENTS WITH JAPAN AND SINGAPORE COULD THREATEN PRIVACY RIGHTS

The European Union has long been considered to have the world's strongest data protection regime, notably since the General Data Protection Regulation (GDPR) entered into application in May 2018, guaranteeing the protection of personal data of Europeans both when their data is processed in Europe and transferred abroad. However, two recently signed trade agreements - with Japan and Singapore - threaten the privacy protections established by the GDPR, and establish a precedent that could weaken the EU's commitment to data protection and privacy.

WHY ARE THE FREE FLOW OF DATA PROVISIONS PROBLEMATIC?

As explained in more detail in a DTA factsheet on data flows, countries may seek to regulate (or limit) cross-border data flows on three major grounds - to ensure the protection of civil liberties (including privacy), to ensure data is accessible to public authorities, and for economic reasons.

Of these, the first is the most relevant to the present context. When data moves across borders, it is subject to a different legal regime. This can be problematic if the foreign jurisdiction offers comparatively limited or no privacy rights to consumers. Companies can seek to evade local privacy and data protection norms merely by moving data to a different location, putting fundamental rights at risk. Accordingly, and as is the case with the GDPR, governments around the world are increasingly implementing legal measures

DIGITAL TRADE ALLIANCE

to ensure privacy rights over data irrespective of its location or in the alternative to stop transfers of personal data to jurisdictions where such protections cannot be guaranteed.

Such legal measures are however under threat from "free flow of data" provisions seen in an increasing number of trade agreements. These provisions primarily aim to promote legal certainty for cross-border digital service provision and therefore to promote economic interests. Due to significant lobbying from Big Tech companies, many recently signed trade agreements contain provisions that limit the ability for governments to regulate cross-border data flows irrespective of the impact on crucial fundamental rights. Any domestic regulation that limits or otherwise impinges on free data flows could be challenged for violating these trade agreements.

The EU, given its high standard of data protection under the GDPR, has typically been wary of entering into trade agreements that may force it to allow unrestricted data transfers to foreign countries or allow other countries to challenge European law that regulates such transfers on grounds of privacy concerns.

However, this position could be undermined by the free flow of data provisions in the agreements with Japan and Singapore.

THE LEGAL BACKGROUND:

The GDPR lays out a comprehensive scheme for protection of personal data of European residents, whether processed in the EU or outside. A key aspect of the protections afforded by the GDPR is that personal data cannot be transferred outside the EU to a jurisdiction that affords inadequate data protection standards.

Article 44 of the GDPR lays out the conditions for export of data from the EU. It prohibits cross-border data transfers beyond the EU unless the EU Commission has found (in an "adequacy decision") that the importing country offers a similar level of privacy protection to the data. Countries that have received adequacy decisions include Andorra, Argentina, Israel, New Zealand, Switzerland, Uruguay, Japan, the UK, and South Korea. Data can thus flow relatively freely between the EU and these countries.

If there is no adequacy decision made with respect to a country, the data controller must ensure the data can be protected through other means once transferred. This can be done through the use of:

I. Binding contractual clauses, an approved code of conduct or by adhering to an approved certification mechanism

II. The presence of a legally binding instrument between public authorities

III. Standard data protection clauses adopted/approved by the EU Commission

Personal data may also be transferred outside the EU in the absence of the aforesaid conditions being met in certain circumstances outlined in Article 49, such as when there is explicit consent of the data subject or the transfer is necessary to fulfill a contract between the data subject and data controller.

In essence, the GDPR attempts to ensure that personal data when moved outside the EU is subject to a similar level of protection as within the EU, including by ensuring that data subjects can exercise their data protection rights.

However, the European Union is also cognisant of the need to ensure greater data flows between countries given the economic benefits this can bring. This can spur cross-border provision of services while also enhancing knowledge flows (thereby promoting crucial fundamental rights such as that of freedom of expression). This clash of competing interests (notably the economic interests of companies and fundamental rights of citizens) is at the heart of recent trade agreements signed between the EU and two Asian countries - Japan and Singapore.

WHAT DO THE TRADE AGREEMENTS WITH JAPAN AND SINGAPORE SAY?

The EU and Japan signed an Economic Partnership Agreement (EPA) on July 17, 2018, with a view to remove various barriers to trade between the countries. While the agreement itself does not contain an article on data flows, Article 8.81 requires the parties to reassess the need for such a provision within a period of 3 years. Subsequent to internal administrative processes, the two countries signed a protocol amending the said EPA on January 23, 2024.

In essence, the protocol bars the signatories from adopting measures that prohibit or restrict the cross-border flows of information. However, the protocol recognises that parties may adopt data localisation measures to achieve a “public policy objective” provided that such a measure is not:

I. arbitrary, discriminatory, or a disguised restriction on trade

II. Imposes restrictions that are proportionate to the objective sought to be achieved

The protocol specifically notes that the parties are not prevented from adopting measures to protect personal data and privacy, provided that the law of the party allows for mechanisms enabling transfers under conditions of general application for the protection of any transferred personal data.

Thus, the protocol establishes a general regime of free flow of data between the EU and Japan, while at the same time ostensibly attempting to ensure that the parties can apply restrictions on cross-border data transfers on grounds of data protection and privacy, as well as other "legitimate public policy objectives" (subject to various conditions).

The EU recently concluded negotiations with Singapore to enter into an agreement on digital trade, which per published draft texts, would contain similar provisions as the Japan-EU data flow protocol when it comes to establishing free flows of data between the EU and Singapore.

WHY ARE THE EU'S NEW DATA FLOW AGREEMENTS PROBLEMATIC?

There are a number of reasons why the data flow provisions in the EU's new trade agreements with Japan and Singapore are problematic.

First, given that the EU already has an adequacy decision in place with respect to Japan, it is unclear why there is a need for a free flow of data provision in the trade agreement between the countries. An adequacy decision permits data flows between the two countries without any further administrative approvals, thereby easing the regulatory burden on businesses that seek to export data from the EU.

Adding a free flow of data provision to the existing adequacy decision does little but further reassure businesses of their ability to continue to export data from the EU. At the same time, it brings with it certain problems. Trade agreements are more difficult to challenge or amend than domestic law or administrative decisions, as they require consensus among the parties to make any changes (while any breach may invite enforcement action under the dispute resolution process established by the agreement). Thus, the EU may find itself in a predicament should any change in circumstance require it to reassess its determination with respect to the level of data protection provided by Japan. While an adequacy decision can be reconsidered internally by the EU, changing the terms of a free trade agreement would require consensus agreement with the Japanese government and would be much more difficult.

At the same time, it is also unclear why the EU is considering free flow of data provisions in its agreement with Singapore, given that no adequacy decision has been made with respect to this country (presumably implying that Singapore does not have a data protection framework that provides a similar level of privacy protections as the EU). A free flow of data clause with Singapore therefore short-circuits the domestic regulatory process established by the GDPR.

Second, while the free flow of data provisions in the two agreements with Singapore and Japan ostensibly seek to protect the ability of the signatories to regulate data flows in public interest, any measure that seeks to restrict data flows must meet the twin tests of being a "legitimate public policy objective" and "proportionality". These tests typically impose extremely high barriers, making it very difficult to justify restrictive measures even if adopted to protect a fundamental right. Not only is there a lack of clarity on what constitutes a "legitimate public policy objective", research demonstrates that of 48 attempts to use "public policy" exceptions (under the general exceptions of the General Agreement on Trade and Tariffs and General Agreement on Trade in Services) to justify domestic regulation, only 2 have proven successful.

Given the fast changing nature of the digital economy, it becomes essential for governments to retain a broad ability to impose new regulations to protect people's fundamental rights. For instance, there may be a need to impose restrictions on data flows in the interests of enhancing cyber security, promoting a competitive digital economy or regulating the AI ecosystem. However, any such measures could be threatened by the free flow of data provisions as seen in the two agreements under discussion, given that every contra measure will have to be justified against unclear and potentially limiting standards.

Third, the agreements do not impose or mandate a minimum standard of privacy to be adopted by the signatory countries. The agreements in fact do not recognise privacy as a "fundamental" right, instead merely recognising the importance of data protection.

Further, while the provisions seen in the two agreements with Japan and Singapore attempt to protect regulatory autonomy insofar as domestic privacy regulation is concerned, this also implies that the adoption of a weak privacy standard by a signatory country cannot be challenged. Thus, the provisions would protect data exports from the EU to Japan or Singapore even if these jurisdictions were to adopt weak data protection laws. It is also unclear how data could be adequately protected if it were to be transferred from Japan/Singapore to a third country, with even lower data protection standards (an issue that has also been highlighted in the context of free flow of data clauses included in

trade agreements signed by Japan with other countries such as the United States). This issue may be exacerbated in the context of Singapore:

I. Singapore is host to a large number of Chinese technology companies (who may transfer EU data to China). Concerns about unethical data processing by Chinese companies have seen countries such as the US implement restrictions on cross-border data transfers.

II. Singapore provides significant leeway to its law enforcement authorities to carry out surveillance and access personal data. Notably, it has no constitutionally recognised right to privacy, with Freedom House noting in its Freedom on the Net 2023 report that the "full extent of the government's surveillance capabilities and practices is unknown." Its personal data protection law too does not apply to the public sector. The (relatively) lower standard of privacy protections afforded in Singapore could therefore be a cause for concern.

Fourth, the protocol signed with Japan enables privacy related localisation measures to be introduced in domestic law as long as they contain derogations (conditions of transfer) that are applicable across the board (horizontally). While there is legal uncertainty on the interpretation of this provision, it could limit the EU's ability to introduce localisation measures in specific contexts, that is, measures that apply to specific controllers or types of data. This may be an issue in the context of data processing that poses a particularly high risk to fundamental rights. It must also be kept in mind that the EU is increasingly using the GDPR to regulate unethical forms of data processing concerned with the AI ecosystem. It may therefore find itself hamstrung when it comes to implementing restrictions on data processing for high risk AI applications/systems.

Finally, it is also relevant to note that trade agreements may not be an appropriate venue to cover issues affecting significant fundamental rights such as privacy. Trade agreements are typically negotiated in secret, without the kind of transparency, oversight, review, and public participation seen in domestic law making and administrative processes. Trade negotiations are also highly susceptible to corporate capture, particularly given their primary objective is to ease cross-border trade in goods and services (as opposed to protecting fundamental rights).

CONCLUSION

While promoting data flows between countries is an important objective, both from a business and civil liberties perspective, it is unclear if trade agreements are the best place

for binding legal obligations to be entered into in this regard. Trade agreements typically seek to open up market access and create legal certainty for businesses. The prioritization of business interests in trade agreements means that they often do not fully take into account possible effects on crucial fundamental rights, such as that of privacy and data protection.

Data flow related clauses, if at all included in trade agreements, must be designed so as to protect the ability to implement domestic public interest regulation particularly of emerging technologies. Fundamental concerns and interests such as that of privacy must not be subsumed by corporate interests in ensuring free cross border data flows.

By enabling free flows of data, without sufficient care to protect fundamental privacy rights of citizens, the EU-Japan and particularly the EU-Singapore agreements could threaten the high standards of privacy that are currently enjoyed by European residents and weaken the gold standard privacy regime established under the GDPR. It is for these reasons that the European Data Protection Supervisor, an independent supervisory authority established under the GDPR, has strongly opposed the inclusion of free flow of data provisions in the Japan agreement (in their current form). A number of European consumer protection and digital rights organizations have also expressed their dissatisfaction both with the content and the process behind the agreements with Japan and Singapore.

In any event, the two agreements with Japan and Singapore should not form a precedent for future agreements with other countries (such as the proposed digital trade agreement between the EU and South Korea), particularly those that may have lower standards of privacy and data protection.

FURTHER READING:

1) European Data Protection Supervisor, Opinion 3/2024, January 10, 2024.
2) Digital Trade Alliance, Cross Border Data Flows and Free Trade Agreements, January 5, 2024
3) Svetlana Yakovleva, Can Japan Have the Best of Both Worlds?, Digital Trade Alliance, 2023
4) BEUC, New EU-Japan data flows article puts consumers fundamental rights at risk, letter to the permanent representation to the EU, November 10, 2023.