ETNO statement on International Data Transfers

July 2023

Introduction

In the last years, new regulatory frameworks that guarantee user privacy in the digital environment have been adopted worldwide, from Africa, to South America and Asia.

The year 2018 marked a turning point in Data Protection with key developments:

- Application of the General Data Protection Regulation (GDPR). The "GDPR-model" has been exported to other jurisdictions around the world.
- California adopted its Consumer Privacy Act (CCPA), which was the first comprehensive State's privacy regulation in the US. It has been followed by similar comprehensive data privacy laws in other nine States[1], while several comprehensive consumer privacy bills are currently being examined in nine more States.
- Brazilian Data Protection Law was passed in August 2018 and entered into effect in 2020.

This trend continues with in Africa, with Kenia having adopted a comprehensive Data Protection Law in 2019 and up to thirty-six (out of fifty-four) African countries having passed Data Protection Laws or Regulations, and in South America, with new Laws in Ecuador, Colombia and important legislatives developments in Chili and Argentina to update their current Laws.

These regulatory developments in different continents have improved the levels of awareness, digital trust and confidence amongst citizens.

[1] Colorado, Connecticut, Indiana, Iowa, Montana, Tennessee, Texas, Utah, Virginia.

Need for horizontal, flexible and technologically neutral frameworks

The development of cutting-edge technologies, such as Artificial Intelligence or the Internet of Things, which are powered by large troves of data to function, is putting to the test the effectiveness of the rules adopted so far. So is their ability to make the territorial borders of States fluid and, with them, opening the door to an increasing exchange of data between countries, citizens, companies and Governmental bodies.

Regulatory frameworks applying to advanced technologies and data governance must have common bases to generate regulatory coherence and simplification, while promoting innovation and privacy protection. For this reason, regulation must be horizontal, technologically neutral, able to evolve in line with technological developments and with a risk-based approach where remedies are proportionate with the risks associated. Therefore sector-specific rules imposing different obligations to basically the same data processing situations, as it is still the case with GDPR and the outdated ePrivacy Directive in the European Union, should be avoided. The GDPR was created to provide a uniform high level of data protection across Europe. The GDPR is technology neutral and its risk-based approach provides a solid basis creating uniform rules for all kinds of processing of personal data and all market participants in the EU. Without prejudice to the continued need to protect the confidentiality of communications, no additional rules need to be maintained with regard to the processing of personal data. The principle “same services, same rules, same rights, same protection” should prevail.

Besides being as much as possible technology-neutral, regulations must be flexible to promote privacy and innovation in a perfect balance between the two. This is very important at a time when Europe wants to lead the way in creating a European model for the exchange and re-use of personal and non-personal data across sectors. As far as personal data is concerned, a healthy and sustainable data economy will not be created if companies remain subject to rigid and obsolete privacy rules, such as the ePrivacy Directive, which penalizes players in the electronic communications sector vis-à-vis internet companies.

Cooperation and convergence: a global issue

Promoting cooperation and the broadening of jurisdictional horizons are essential to achieve a more homogeneous privacy and data protection framework. We cannot forget that the right to privacy is an internationally recognized Human Right and must

therefore be guaranteed worldwide. If data know no borders, the convergence of the regulatory frameworks governing them must also include this global aspiration.

This issue is particularly relevant to ensure a cross-border flow of data that sustains and promotes digital commerce, with the guarantee of compliance with privacy regulations while respecting the Fundamental Rights of users and citizens. In this direction, national Constitutions of very different countries worldwide have explicitly enshrined privacy as a Fundamental Right.

Therefore, it is important for the European Commission to update the small number of pre-GDPR Adequacy Decisions that recognize an adequate level of protection in certain countries (e.g.: Switzerland, Argentina, Uruguay, New Zealand…), based on the GDPR and the jurisdiction of the Court of Justice of the European Union. In addition, the Commission needs to engage with countries that in recent years have endowed themselves with new Data Protection Laws and institutional structures (independent National Data Protection Authorities) to ensure that these countries also guarantee an adequate level of protection. Asia, Latin America and Africa are geographical areas that the Commission should explore with attention, considering their dynamism in data protection in recent years.

Stronger convergence with other regions of the world would also benefit EU competitiveness, by reducing market barriers and facilitating foreign investment and trade. The creation of free data flow areas based on seamless privacy safeguards is increasingly recognised as a key pillar of the European Union's economic cooperation with third countries, as recent Adequacy Decisions with Japan and South Korea show.

Interoperable regulatory frameworks across jurisdictions to guarantee an open and secure digital world

Considering the remarkable size of the data flows between the United States and the European Union, the two regions must also cooperate to ensure that data transfer respects democratic values and principles. The new data adequacy decision for the EU-US Data Privacy Framework that entered into force on 11 July can be of vital importance to guarantee the adequate protection of the privacy of individuals on both sides of the Atlantic. Ahead of the adequacy decision, US government has completed the implementation of additional measures, such as the creation of a data protection review court, to address some of the concerns raised by the European Court of Justice in its jurisprudence ('Schrems II' ruling). It is important that the application and enforcement of these rules is closely assessed and monitored so that the new EU-US Data Privacy Framework can indeed bring lasting regulatory certainty for transatlantic data flows.

The renewed momentum for international cooperation and the opening of spaces for reflection and collaboration represent a unique opportunity to look to the future and to put effective privacy and data protection in action. A stable and durable data flow model

that guarantees privacy and data protection in the long term and is innovative in the economic sphere is key to reaping the benefits of the digital ecosystem and mitigating potential risks.

Concluding remarks

We hope that these reflections will help to build a more uniform, coherent, interoperable privacy and data protection framework, based on European values, the respect for fundamental rights, and the high standard set by the GDPR. All stakeholders, Public Administrations, policy makers, Data Protection Supervisors, private companies, civil society and individuals, should commit in this joint endeavour. Only with such a joint effort, it will be possible to face the technological and business complexity we are living in, providing certainty and viable, agile and flexible solutions that can adapt to these dynamics. This is even more true considering that these solutions are aimed at protection the Fundamental Right to Data Protection.