Information Sharing 2.0: tackling the privacy and cybersecurity challenge

It is widely recognized that sharing actionable information – information about vulnerabilities, malware indicators, and mitigation measures promotes cybersecurity. As cybersecurity law and policy has evolved, questions have been raised about the privacy implications of information sharing among organizations and between them and CSIRTs. Certain legislative texts such as the EU General Data Protection Regulation and the US Cybersecurity Information Sharing Act of 2015 tackles this uncertainty directly, by clarifying the conditions under which such information sharing is allowed. Still, there remain unanswered questions about the collection, use and sharing of such information, in light of heightened sensitivity to privacy protection in recent years.

The aim of the discussion is to explore the intent and effects of leading legislative texts such as the GDPRand the CISA rules, in search of examples of balanced legal rules that can promote both cybersecurity and data protection.

Drawing from the best practices put forth by the participants and comments from the audience, the panel will deal with the intent and pragmatic deployment of these and similar rules. The experiences shared can hopefully inform the global cybersecurity-privacy conversation for the benefit of stakeholders - CSIRTs, law and policy makers, privacy professionals and private companies - across the globe, in designing legal rules in this area.

.

The international community, by being receptive to such input, could enable the development of better global interfaces between domestic policies to enhance cybersecurity. Such an approach can constitute a fertile terrain for effective international conversations on cybersecurity to take place.

<u>Guiding questions:</u>

- What were the underlying considerations and legal factors behind the relevant provisions of the GDPR, CISA and other relevant legislative texts?
- In practical terms, how have these provisions been understood and implemented by the private and public sector in the context of cybersecurity?

- A majority of the processing activities in the cybersecurity context is focused on machines and not on their users, and the data collected is mainly technical. How does that affect the analysis of applicable data protection laws?
- What are the main lessons for developing cyber law and policy?
- What are the main issues to take into account for global interoperability in this area?