Aspen Cyber Summit

Keynote Andrea Jelinek: A New Era for Data Privacy

8 November, 13:15-14:00

California Academy of Science

55 Music Concourse Dr, San Francisco, CA 94118

Dear ladies and gentlemen,

It is an honour for me to attend this meeting with some of the most influential voices on cybersecurity.

Today, my aim is to shed light on how the implementation of the General Data Protection Regulation has unfolded and on the state of play of cyber security measures in Europe.

The GDPR represents the most significant change in the European data protection regime since the approval of the Data Protection Directive, over 20 years ago.

In Europe we have opted - with the GDPR - for one overarching law rather than sectoral rules. These "common rules of the game" create a level playing field and ensure that data can move easily between operators, while guaranteeing the consistent protection of individuals' personal data. The goal is to have one set of privacy rules that are interpreted in a uniform way throughout the continent.

The GDPR has at its heart the principle of accountability and relies heavily on businesses' capacity to self-regulate. Organisations are responsible for complying with the GDPR and must be able to demonstrate their compliance. This is an important idea to bear in mind and I'll come back to this later when I discuss the interplay between the GDPR and cybersecurity legislation in Europe.

The GDPR ensures the protection of personal data and obliges organisations to prevent - by the implementation of adequate security measures - data breaches and to report breaches within a given deadline, with much higher fines than it was the case in the past to ensure compliance. The EU has supplemented the framework with a Directive specifically intended to fight hackers and combat cybercrime.

Almost at the same time as the GDPR entered into application, EU member states had to adopt national laws to implement the European Directive on Security of Networks and Information Systems, the so-called NIS Directive.

This NIS Directive harmonizes the rules on cyber security in the EU Member States. It establishes an EU-wide platform to share and exchange information between the Member States. A network of national Computer Security Incidents Response Teams (CSIRTs) brings together the national authorities.

Together with the GDPR, the NIS Directive has an important impact on many organizations. For the first time, we now have an information security regulatory framework with national authorities and European-wide information security standards.

The GDPR is based on the privacy by design principle. This principle states that any product or service shall be designed from the very beginning with data minimization standards in mind. Therefore, organizations shall limit the processing of personal data only to what is strictly necessary

for the purpose for which the data is gathered. Access to such data shall be limited to those who need it for the execution of their duties.

Consequently, companies should assess, on a recurrent basis, whether the technical and organizational measures implemented are enough to provide sufficient warranties to avoid any data breach or leakage.

From a GDPR perspective, organizations are expected to assess whether the processing activities and the potential risks for data subjects resulting from those activities are covered by the security measures in force. Here I come back to the core principle of accountability. The GDPR does not state which specific security measures or which minimum technical standards are sufficient. Instead, it obliges organizations to assess and decide themselves what type of measure shall be implemented in order to comply with the GDPR and to avoid by all possible means cyber security breaches or data leakage.

If despite all precautionary measures a data breach takes place, the Member States Supervisory authorities, gathered in the European Data Protection Board, are competent to verify the security measures put in place by the organisation where the breach took place. If the measures are found to be lacking the authorities can issue warnings, impose a ban and eventually impose a fine up to 2% for lack of reporting data breaches and up to 4 % for inadequate precautionary measures.

The General Data Protection Regulation, states that personal data breaches must be notified to the relevant supervisory authority no later than 72 hours after the data controller becomes aware of such a breach. In this regard, the NIS Directive also imposes a duty on companies to report cyber security breaches to the relevant competent authority at a national level. The competent authority has the obligation to work in close cooperation with the data protection authorities.

The volume of digital information in the world doubles every two years, artificial intelligence systems and data processing deeply modify our way of life and the governance of our societies. The likelihood of being subject to a data breach increases every day.

If we do not modify the rules of the data processing game with legislative initiatives and if we do not combat cyber crime with far-reaching measures, it will turn into a losing game for the economy, society and for each individual.

Compliance with data protection regulations can help to be prepared or well-equipped in case of a data breach. This is a crucial factor in gaining and retaining consumer trust. Trust has always been at the core of the economy and this is more true than ever before in today's digital society. The GDPR, together with The NIS Directive, enable a more functional information economy with more transparency for citizens and a beefed-up cyber security network, which should lead to more trust.

Combating cyber crime and strengthening cyber resilience are key for economic and social development. It is crucial that in doing so, we find the right balance between democratic rights and national security. I look forward to learn more today about the state of play of Cyber security legislation in the US and to discuss with you how we can learn from each other's experiences to ultimately become better at confronting cyber threats.