GLOBAL ONLINE TRAINING

Protecting Data Privacy in the Private Sector in Times of Covid-19 – Key Takeaways

#DataProtection #PrivateSector #GlobalPerspective

Thursday, 09 July 2020

The current Covid-19 crisis is forcing businesses to switch to digital formats under enormous time pressure. Existing tools are being rampantly used and new ways of virtual communication are emerging. This rapid rise of digital tools has made companies vulnerable to the risk of violating privacy rights. The question remains on how they can most effectively ensure the data protection, especially in the current situation. You can find the full online training here.

Speakers:

- Carlos Hernández, International Cooperation Expert, Mexico (moderator)
- Dr. Patricia Peck Pinheiro, Head of Digital/Cyber Law, Pires & Gonçalves Advogados Assoc., Brazil
- Dr. Christian Schefold, Partner, Dentons, Germany
- Frank Abdulai Iddrisu, Financial Crime Investigator, Fidelity Bank, Ghana
- Srinivas Poosalra, Chief Privacy Officer & DPO (Worldwide), Infosys, India

Data Privacy challenges

- Working from home increases the risks related to data privacy and cybersecurity: hackers and other criminals can access private networks often due to human error.
- Non-electronic data (i.e. written on paper) can be easily compromised before being digitalised, which generates a trade-off between (de-centralised) data security and prevention effectiveness.
- The time required to create measures for data protection and cybersecurity is often underestimated.
- In some countries, such as India, systematic and dedicated data protection and cybersecurity laws have been introduced fairly recently, without training or best practices being shared; this poses a challenge for multinational enterprises and even more so for small and medium enterprises, thus there is a need to accelerate information sharing on best practices especially now that resources are more scarce.
- In General Data Protection Regulation (GDPR) compliant environments, employers have the challenge of not being allowed to obtain and use health-related data of their employees, so in practice, data privacy has to be weighed against health risks.
- Employees may not be sufficiently trained to engage with cutting-edge technology and current data privacy provisions.

GLOBAL ONLINE TRAINING

Protecting Data Privacy in the Private Sector in Times of Covid-19 – Key Takeaways

#DataProtection #PrivateSector #GlobalPerspective | Thursday, 09 July 2020

Best practices

- ISO 7001 can either be used directly or as a guidance for sector-specific regulations safeguarding cybersecurity.
- The German contact tracing app (Corona-Warn-App) seems to present a best practice in the compromise between data privacy and useable health information.

Recommendations

- Transparency regarding the use of citizens' data is key (how is it collected, how is it stored, how is it used) to promote both acceptance and data security.
- Governments should not only introduce new and improved regulations but also provide tools to implement them (including dedicated loans).
- International and global approaches, including treaties between nations, should be favoured vis-à-vis national approaches.
- Academia can promote a change in culture by explaining the practical meaning of issues like data privacy and anonymisation and spreading knowledge among relevant practitioners and business representatives in a free manner.
- Companies should provide employees with quick and practical support to deal with cybersecurity issues and stay vigilant.
- Companies should have a structured overview of their data architecture and the different privacy requirements of different datasets so that they can implement the necessary data privacy and cybersecurity safeguards.