

Data Privacy Day 28th Jan, 2017

Celebrated in India under the leadership of Data Security Council of India

... join the industry voice to build stronger Data Privacy Regime

CEO MESSAGE

January 28, 2017

Dear Friends,

It's my pleasure to write to you on occasion of Data Privacy Day (DPD). Year on year, the privacy landscape continues to get more vibrant. In 2016, we witnessed significant developments in privacy space. Many global organizations faced geographical shut downs such as WhatsApp shut down in Brazil, LinkedIn being blocked in Russia, gaming apps such as 'Pokemon GO' not getting access in many geographies, etc. Facebook's decision to integrate its services with WhatsApp faced censure from European Regulators. Apple went public against FBI with its position on not compromising privacy of consumers, opposing enablement of access to a locked device. Microsoft won interim court decision against the US government which required them to share personal information of US citizens stored in servers in Ireland. These incidents and more kept privacy discussions fresh and alive across the world.

Cross border data flow agreements are being challenged and undergoing an evolution. After the invalidation of EU-US Safe Harbor agreement in October 2015 by Court of Justice of the European Union (CJEU), the EU Commission and US DoC came up with a revised framework 'EU-US Privacy Shield', in July 2016, as a legal means to transfer personal information between the EU and US businesses. The legality of Privacy Shield was threatened after it was further challenged for its legitimacy to satisfy concerns around mass surveillance by the US government. Recent executive order by US President Donald J Trump to exclude foreign citizens from scope of Privacy Act of 1974, and exclusion from Data Privacy policies of US government agencies has reinvigorated Privacy concerns by the EU and puts a cloud of uncertainty around Privacy Shield. The Irish Data Protection Authority meanwhile also challenged the legitimacy of Model Contracts as an instrument for cross border data flows.

In 2016, the EU finalized General Data protection Regulation (GDPR) to be enforced starting May 2018. With its stringent requirements and granular prescriptions, Industry is assessing the challenges and cost of doing business in conforming to GDPR. Regular guidelines are being released by Article 29 Working Party on various aspects being discussed in GDPR. Apart from EU, new privacy laws/frameworks are being formulated by many other major geographies and states, such as US FCC adopting privacy rules for Broadband players, Russia updating its status on Data Localization Law, Japan amending its Act on the Protection of Personal Information (APPI) and releasing its enforcement date for May 2017. In order to deal with rising privacy concerns, some of the US states such as Washington, West Virginia, Ohio, Arizona, etc. have started hiring Chief Privacy Officers to ensure safe organizational practices of processing personal data. Numerous surveys have also revealed that individuals, inadvertently or otherwise, continue to compromise their privacy while using certain websites and social media platforms in return for free services and better user experience.

On the Indian turf, a law to regulate use of Aadhaar was enacted. It tries to address privacy related concerns through certain provisions, however many are raising concerns on inadequacy of the provisions. We were also earlier hit by a malware incident impacting debit cards used in ATMs. Towards the end of the year, sudden transition towards a 'Less

Cash' society triggered a slew of digital applications and services made available by not only digital wallet providers, but also nationalized banks. Volume of e-wallet transactions have skyrocketed by 271% in a month; value of such transactions also rising by 267%. It has also fueled the concerns on cybersecurity and privacy risks associated with such transactions, and concerns if security and privacy by design were factored in during application and services design, given the pressure to churn out payment products and solutions rapidly. On the positive side, the Indian service providers are developing the understanding of EU GDPR as to identify their applicability while conducting business with EU organizations. The Indian outsourcing industry is focusing on implementing and operationalizing the applicable clauses of EU GDPR or the ones which may be pushed by EU organizations (data controllers) through contracts after May 2018.

DSCI has been working with Government agencies and industry representatives to strengthen the cyber security and data protection regime of the country. We continuously keep taking initiatives to promulgate privacy and its importance in today's scenario. Some of the large organizations in banking and telecom space have embarked on Data Privacy journey, and are designing and implementing their privacy program based on [DSCI Privacy Framework \(DPF©\)](#). Through our [DSCI Certified Privacy Lead Assessor \(DCPLA©\)](#) and [DSCI Certified Privacy Professional \(DCPP©\)](#) certification and training program, individuals and corporates are getting trained on privacy. The community of certified Privacy Professionals has had an impressive growth last year. To cater to rapidly changing Privacy requirements, we have undertaken curriculum revision to make DCPP© up-to-date and relevant. The privacy community interaction has been phenomenal – some tough questions drawing equally knowledgeable responses from experts. It is the collective knowledge that pushes up our Privacy quotient.

With Industrialization 4.0, IoT getting mainstream and rapid digitization, data generation and processing will increase manifold. Rising expectations on privacy will warrant nation states to adopt laws and regulation to maintain interoperable data flow framework. DSCI is proactively working on elevating the importance of cross border data flows in trade negotiations and continuously advocating enactment of comprehensive Privacy law in India. DSCI also participated and hosted numerous discussions on topics related to data privacy subject across India last year.

[Data Privacy Day](#) presents us an opportunity to comprehend the changing scenario, and think about ways of reaching out to consumers and end-users on one hand; and to corporates and policy makers on the other. Chapter meetings pan India have been scheduled and discussions are held on topics relevant to data privacy and other contemporary issues that impact the privacy of individuals.

I look forward to your enduring support in making this day and the whole concept of Data Privacy a success, and getting India recognized as a leader in privacy protection in the world.

Rama Vedashree
CEO, Data Security Council of India

References:

[IBM.com](#) [privacysheild](#) [computerworld](#) [time.com](#) [panamapapers](#) [digitaltrends](#) [bbc.com](#) [statetechmagazine](#)

