Image courtesy
DSCI

## On Data Privacy Day, some industry perspectives

**Today, January 28 (2022) is celebrated as Data Privacy Day (DPD) across the world.The objective of the day is to sensitize individuals and disseminate privacy practices and principles. It encourages everyone to own their privacy responsibilities to create a culture of privacy.**

**The theme for this year is 'Privacy Matters'**. It instils a sense of accountability that Privacy is integral to every individual's life. We must become conscious towards it and be more responsible towards our data – as after all #PrivacyMatters.

We bring you some industry perspectives below.

**A.S. Rajgopal, Founder, MYn App:** *"I urge all media organisations, government agencies and my fellow citizens to lift up their voices against violation of data privacy, which is a pressing issue in today's times. Privacy is a fundamental right. It is my fundamental right and your fundamental right. Let's come together and claim what's rightly ours. Join me in this nation-wide social media blackout on the 28th of January from 5 to 6pm, this Data Privacy Day.*

MYn, an app that functions on 100% privacy and zero targeted advertisements was launched to disrupt the contemporary social media, commerce, and workplace landscape, is an advocate for Right to Privacy. This hour-long social media pause, is a silent protest against all forms of privacy and data violation occurring in our day-to-day social media environment. Switch off from all social media applications from 5 to 6 PM, on January 28.

**Nikhil Arora, Vice President, and Managing Director, GoDaddy India**: In today's digitally-driven world where cyber-crime and data theft are rising at an exponential rate, the need for small business owners to pay more attention to security protections for their online business becomes more critical. While bigger corporations are working towards upgrading their data protection ecosystem, small businesses are finding it hard to invest in the right technologies needed to help safeguard their business and customers' data, often making them more susceptible to privacy breaches. Indian businesses need to analyze the potential risks and develop a data-protective attitude, which not only helps in securing sensitive customer and business data but also enhances the customer experience. At GoDaddy, we will continue to create awareness around it through our suite of website security tools and solutions. We believe a strong impetus by India's small business owners to more actively work to protect the data they collect could aid in securing more

trust in their businesses. We are confident that working together in India will accelerate its focus and work towards creating a more safe online ecosystem in India

**Rajesh Ganesan, Vice President, ManageEngine**:As the union government gears up to introduce laws to protect consumer data, organisations should bear the onus of educating their employees. Data protection is only successful when all components within the infrastructure—including all employees—are prepared to handle it. To do this efficiently, data protection must be built right from the design stages of all services and operations. It should be present as a strong, invisible layer. It is best to educate employees on the do's and don'ts of data protection in a way that is contextually integrated into their work, as opposed to relying solely on periodic trainings. Given the forthcoming legislation, corporate data management is more important than ever, and it's up to business leaders to create the teams, structures, and expertise to keep all their corporate data well-protected and staying compliant in 2022.

**Ripu Bajwa, Director and General Manager, Data Protection Solutions, Dell Technologies, India:** Data Protection Day serves as a global reminder for one of the most important responsibilities of any organization, which is to keep sensitive and mission-critical data secure. Today, many organizations in India and around the globe are exposed to sophisticated vulnerabilities, as their infrastructure and data security framework is inadequate. Malware, ransomware and cyber threats have become more specialized and penetrative. Once a lapse is identified, attackers can misuse the data and create situations in which data, once lost, may not be recovered.With the hybrid work model, organizations also process complex amounts of data in environments where frequent exchange of data may occur from multiple touchpoints. The influence of emerging tech like cloud-native applications, Kubernetes containers, and AI in day-to-day business activities also increases the risk of misuse of data due to the lapse in the upkeep of cybersecurity goals and IT infrastructure, making organizations vulnerable to cybersecurity threats.

**Kumar Vembu, CEO and Founder, GOFRUGAL:** It's time to understand what freedom means, mainly digital freedom. We leave our digital trails whenever we engage digitally. Algorithms have started using the data to condition our minds, influence, and sometimes even dictate what we should be doing in the future. Data protection is all about freeing ourselves from digital slavery. The goal of data protection is to give power to the data owner. It is the capacity to decide what data should be stored, how it should be used or not used, and to make sure they don't end up as slaves to the machines.

**Sundar Balasubramanian, Managing Director, India, and SAARC, Check Point Software Technologies:** Data Privacy Day, is the perfect time for individuals and businesses to evaluate their data hygiene and security protocols to ensure their data is kept as safe and secure as possible. Check Point Software is beginning 2022 with a new strategic direction that follows the mantra: You Deserve the Best Security. While adopting the kind of best security practices promoted by Data Privacy Day is vital, it's only a baseline. We know that businesses can't afford to settle for second best when it comes to defending themselves in a constantly evolving threat landscape. That's why we're working hard on cutting-edge technologies such as our recently announced Quantum Lightspeed firewalls, and why each and every one of our software solutions are powered by our global real-time threat intelligence platform.

**Sumit Srivastava, Solutions Engineering Manager – India at CyberArk:** It's not just humans that are susceptible to clicking on the wrong link or are perhaps a little too cavalier about what they share about themselves. Software bots have sharing issues too, and this Data Privacy Day we highlight how we can better protect the data that they access from being exposed.Software bots – little pieces of code that do repetitive tasks – exist in huge numbers in organizations around the world, in banking, government and all other major verticals. The idea behind them is they free up human staff to work on business-critical, cognitive, and creative work, but also helping improve efficiency, accuracy, agility, and scalability. They are a major component of digital business.. The privacy problem arises when you start to think about what these bots need so they can do what they do. Much of the time it's access: If they gather together sensitive and personal medical data to help doctors make informed clinical predictions, they need access to it. If they

need to process customer data stored on a public cloud server or a web portal, they need to get to it. We've seen the problems that can arise when humans get compromised and the same can happen to bots – and at scale. If bots are configured and coded badly, so they can access more data than they need to, the output might be leaking that data to places where it shouldn't be.

**Lana Xaochay, Data Privacy Officer, US based technology company Ivanti :** When the World Wide Web launched in the public domain on April 30, 1993, no one realized the sheer amount of personal information that would be stored and shared online. According to the World Economic Forum, it's estimated that by 2025 there will be 463 exabytes of data created every day! This poses a challenge for organizations as managing data has become increasingly complex and governments around the world have tried to rein in what and how we share and store data.

Data privacy concerns have been exacerbated by the pandemic as we have seen an uptick of ransomware and cybercrimes with bad actors taking advantage of the rapid shift to remote work, the increase in online deliveries and the proliferation of QR codes. The sheer amount of data we share about ourselves online is a privacy concern and more alarming is that many workers are using the same devices for personal and business activities. For this reason, it is critical for businesses to be able to manage all devices that access their network, along with effectively prioritizing and remediating vulnerabilities that pose the most danger to their organization.

**Tim Mackey, Principal Security Consultant, Synopsys Software Integrity Group**: When there are options to purchase an item or service, brand reputation is a key element in the selection process. Effectively, the purchaser expects delivery of a quality product and that the supplier will stand behind their products and be there should support be required. Since the majority of business activity involves personal data – even to the degree of a simple credit card transaction in a shop – businesses who fail to properly manage the data their customers willingly share risk damaging their reputation and by extension break the trust their customers have placed in them.

**Andy Teichholz, Global Industry Strategist, Compliance & Legal at OpenText:** Data privacy reform has changed our global community forever. As we begin 2022, organisations face an emboldened world demanding greater accountability and trustworthiness. The recent steps taken by several countries to bolster their consumer privacy rights and processing activities (such as China's Personal Information Protection Law) will have a far-reaching global impact on privacy rights and data protection practices. People are more empowered than ever to exercise their rights, submit Subject Rights Requests (SRRs) and reclaim control of their information. They want to understand how their data is used and to access, correct, delete, and restrict use. To meet these data-intensive demands and overcome a scarcity of resources to support key business activities, organisations must embrace process automation for SRR response and apply case management tools that best track its performance and effectiveness. A well-executed program that delivers a strong experience will be critical to improve customer satisfaction and loyalty.

**In our Image of the Day spot, we feature a Privacy glossary created by *Digital Security Council of India, a* not-for-profit, industry body on data protection in India, setup by NASSCOM**