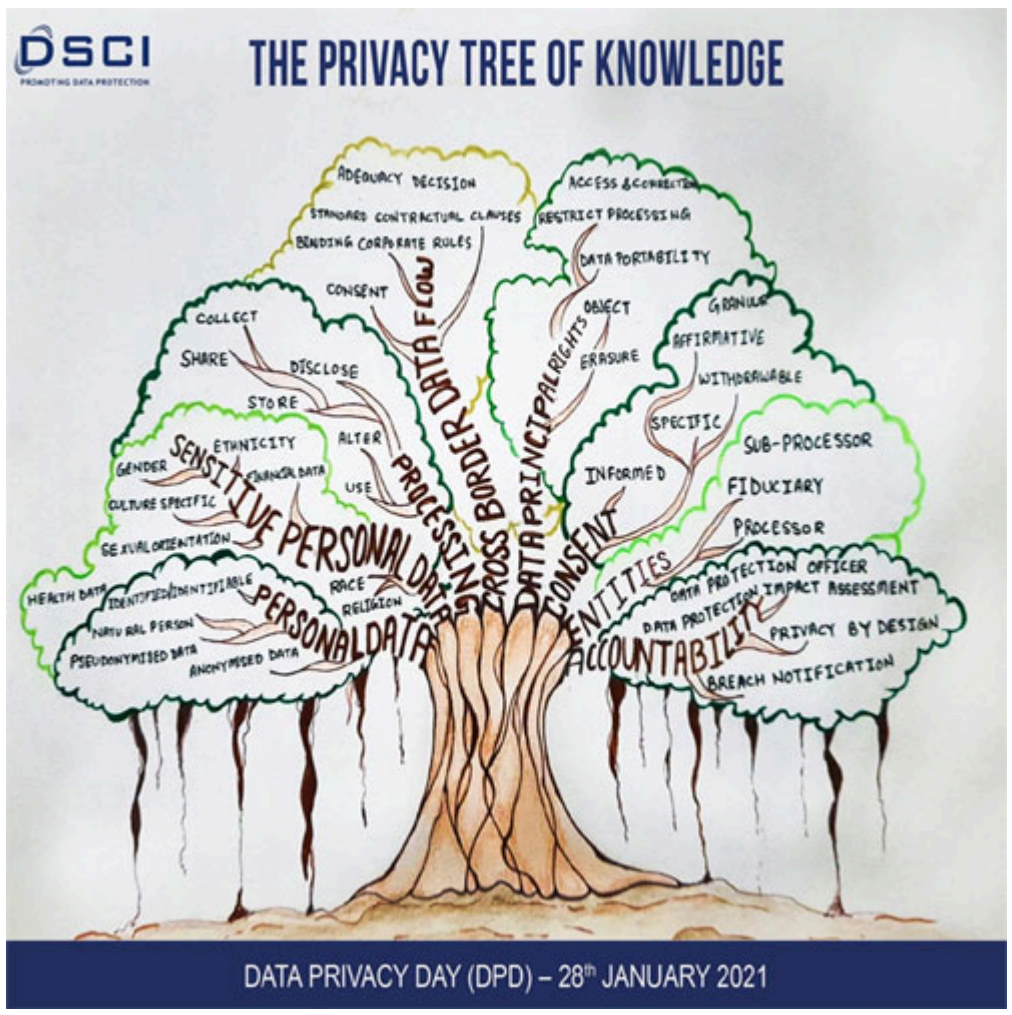
VARINDIA

Data Privacy Day is an effort to safeguard data and enable trust

by VARINDIA 2022-01-28



Millions of people are unaware of and uninformed about how their personal information is being used, collected or shared in our digital society. **Data Privacy Week** is an international effort to empower individuals and encourage businesses to respect privacy, safeguard data and enable trust. January 28 is celebrated as **Data Privacy Day (DPD)** across the world.

Cybercrime as a service is a huge thriving industry in itself. The picture you imagine of a single hacker sitting behind his computer screen is of the past now. 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.

To celebrate this year's DPD, apart from the Privacy collaterals, we also have data privacy experts for a morning talk and panel discussion on data privacy developments and innovations in privacy technology, along with the launch of CyberShikshaa "Women on Break" privacy module.

It is heartening to see the interventions that are being planned world over to promote the protection of personal data. Domestically, the country's journey towards its first Privacy legislation marched ahead with various stakeholders from different quarters deposing in front of the **Joint Parliamentary Committee**. The JPC is expected to table its report in the Parliament in the budget session. In addition, the discourse around the framework for Non-personal data is also receiving substantive attention.

For Individuals: Own Your Privacy

Personal info is like money. Your purchase history, IP address, or location has tremendous value. Make informed decisions about whether or not to share such data with certain businesses.

Keep tabs on your apps. Delete unused ones and keep others secure by performing updates.

Manage your privacy and security settings. Continuously check them to limit what information you share.

For Businesses: Respect Privacy

If you collect it, protect it. Make sure any personal data you collect is processed in a fair manner and is only collected for relevant and legitimate purposes.

Consider adopting a privacy framework to manage risk and secure privacy within your organization.

Asses data collection practices by evaluating which privacy regulations apply to your organization.

Transparency builds trust. Be honest with customers about how you collect, use, and share their personal information.

Maintain oversight of partners and vendors. You are responsible for anyone collecting and using your consumers' personal information.

"Toward the end of 2021, **Check Point Research** noted that cyber-attacks against corporate networks had increased by a staggering 50% on the previous year. The education and research sector was the hardest hit, averaging 1,605 attacks per week, with government organizations, communications companies, and internet service providers close behind. Even attacks on the healthcare sector were up 71% on pre-pandemic levels, showing nothing is off-limits to threat actors. In our 2022 Security Report, we also noted that email had become an increasingly popular vector for distributing malware throughout the pandemic, now accounting for 84% of malware distribution. Beyond the corporate world, it was also clear that large-scale attacks on critical infrastructure, such as the Colonial Pipeline incident, had a very real impact on people's day-to-day lives, even threatening their physical sense of security. Data Privacy Day, or Data Protection Day as it's known in Europe, 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."- Says **Sundar Balasubramanian, Managing Director, India, and SAARC, Check Point Software Technologies**.

Ripu Bajwa, Director and General Manager, Data Protection Solutions, Dell Technologies, India says, "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.

Consumers are also constantly discovering the information that is collected about them, how that data is used, and how daily breaches put that information at risk. Consequently, organizations must make security a top priority to maintain consumer trust and remain compliant with regulations. To address these challenges, a few steps that organizations must take, include, an accurate inventory of data. This is critical for adhering to data privacy regulations, such as GDPR. Many organizations may not know the information they have or where it is going, thereby making it difficult to protect it. Additionally, solutions that dynamically allow or deny access based on contextual factors like a user's location, device type, or job function are highly favorable, along with data loss prevention (DLP) capabilities. India is also taking steps to implement a data protection framework that incorporates many elements of the GDPR. Ultimately, in today's highly regulated data environment, Indian organizations need to adopt and build effective compliance strategies to achieve business value. Organizations with low levels of data protection and data governance frameworks need to change quickly."

Andy Teichholz, Global Industry Strategist, Compliance & Legal at OpenText on Data Privacy Day says, "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."

Sumit Srivastava , Solutions Engineering Manager – India at CyberArk says, 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.

A.S. Rajgopal, Founder, MYn App said, "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."

Ravi Chhabria, Managing Director, NetApp India

Data used to be a by-product of business. Every organisationbusiness recorded transactions, stored product, process, customer records, during the normal course of conducting business. The sea change in the past few years, is that with deep tech, vast amounts of telemetry, AI, ML, analytics, businesses are being built on data. Data is creating value. Data is the business. Data is the source of competitive advantage. Data also gives rise to risks involved. In addition to traditional risks, there is is are also the ongoing risks of ransomware, denial of service (DoS) and, theft of intellectual property. No wonder, data protection and security have become core to businesses.

Beyond the headline-grabbing numbers, there remain core principles sensible organiszations must observe. Above all else, good security management is predicated on good data management. Along every step of the security journey – from prevent to detect to respond – knowing where your data is, how to extract it, and how it interoperates across and beyond organizsational boundaries are key to ensuring you protect yours and your customers' most valuable intelligence. With data privacy regulations and requirements growing more complex, users must look at solutions that simplify compliance in encryption and sophisticated AI that maps and classifies data.

Nitin Varma, Managing Director, India & SAARC, CrowdStrike

“Over the last 2 years, there has been a significant rise in cyber-attacks all over the world. The pandemic has increased our dependency on mobile devices and remote access to core business functions. While remote working became the saviour, it also introduced a new set of security challenges by raising concerns regarding identity-based threats, privacy breaches and the loss of essential data from unprotected devices and systems. Despite the best efforts of security teams, attackers consistently took advantage of vulnerabilities, discovering new ways of infiltration and taking advantage of people’s curiosity as well as their fears around Covid, leveraging socially engineered lure files and tactics.

There is a huge digital shift that has been created by the pandemic where many industry sectors have witnessed an accelerated approach towards digital transformation and their erstwhile perimeter has moved beyond their enterprise firewalls to cloud; either a public cloud, hybrid cloud or a private cloud. This has added complexity to the IT architecture stack and also increased the potential attack surface for adversaries to exploit; and often under-resourced security teams to protect.

Today’s new perimeter needs to be buttoned up with operations and security collaborating to create a secure network. With more data moving to the cloud every day, it is imperative to have a re-architecture of the cyber strategy which should go around all three dimensions of security i.e. people, process and technology.

While many cloud service providers offer basic levels of data security, it is critical for organizations to develop and implement a comprehensive data security strategy that’s scalable and combines automation with human threat hunting and threat intelligence. Another critical element of a data security strategy is real-time monitoring, detection and response. These threat detection and response capabilities should be supported by machine learning and analytics to better identify anomalies and malicious activity.

Companies require proficient and skilled cyber security experts who can keep their endpoints, cloud workloads, identify and data secure. Unfortunately some organizations still rely on legacy security solutions that are just not fit for purpose especially as adversaries evolve their tools, techniques and procedures (TTPs). They need security that is scalable, built for the cloud and can carry the same level of control and visibility from their on-premises environment into remote working environments.

Meeting these challenges head on with a layered, unified approach to security will enable organizations to move forward with their cloud plans with the knowledge that their users and data are well guarded.”

Sandeep Bhambure, Vice President & Managing Director, Veeam India & SAARC

“Data privacy has become a high priority for corporations across India, owing to factors such as increased global business operations and outsourcing of work to specialists outside of the organisation. Furthermore, the increased adoption of hybrid working models has made data maintenance and security more difficult. The significant increase in digital convergence has made it possible to easily exploit data beyond the stated intentions. This has added additional responsibility on organizations to protect the personal data of its employees and customers. Gartner predicts that by 2024, worldwide privacy-driven spending on data protection and compliance technology will exceed USD 15 billion annually. The Indian Government too has proposed a data protection law for data privacy assurance to support the ongoing issue around data privacy breaches. These standards seek to provide a privacy assurance framework for organizations to establish, implement, maintain and continually improve their data privacy management system.”

Kumar Vembu, CEO and Founder, GOFRUGAL says, ““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.Data protection means empowerment to the consumer so that they have the freedom of choice every time they shop. It is about establishing a level playing field and healthy

competition in business. Most importantly offer a guarantee about the security and safety of personal and business data.On this data protection day, let us commit ourselves to understanding our rights to enjoy our freedom as digital citizens. This Data Protection Day is a global reminder for organisations, governments and regulatory bodies alike to upgrade themselves to suit the demands of digital age.

Finally, Privacy is Power. Protect it. Remember, not everyone deserves a seat at the table of your life...