TATA CONSULTANCY SERVICES

Building an Intelligent Data Privacy Culture: The Smart Way to Improve Compliance

WHITE PAPER

Abstract

As countries across the world strengthen data privacy regulations and individuals gain more control over the use of personal data, larger organizations are challenged with the execution and implementation of data privacy regulations. According to Cisco Data Privacy Benchmark Study, only 59% of companies are meeting GDPR requirements today[1]. As data privacy becomes critical to enhance customer experience and drive greater value from data assets, taking a tactical approach towards enhancing data privacy maturity is a must.

This paper outlines a phased approach to create a successful data privacy program -- one that helps assess the current data privacy posture, strengthen data building blocks for readiness and implement technology to automate the key tenets of data privacy such as consent lifecycle and data subject rights.

[1] *Cisco.com, Maximizing the value of your data privacy investments, January, 2019, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf ,accessed on January,21, 2021*

How regulations impact data privacy management

Penalties of nearly EUR 300 million have been imposed on more than 400 organizations for non-compliance towards GDPR and similar data privacy and protection regulations in 2019-2020 (see Figure 1).

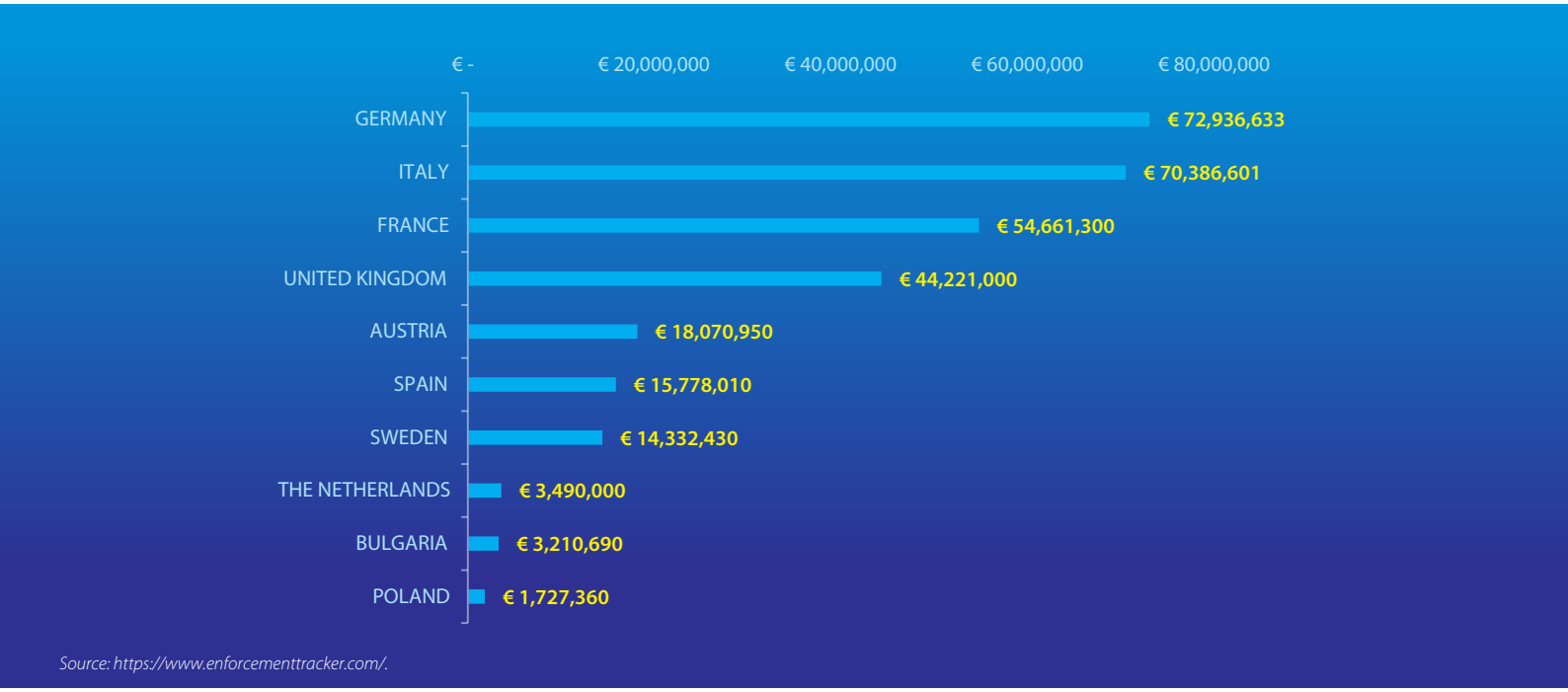

Figure 1: Top 10 countries that saw GDPR non-compliance penalties

With dozens of regulations becoming the law in 2020, the implications and penalties on organizations are predicted to be four- to five-fold as compared to GDPR. The solution lies in a centralized and digitized approach that helps automate consent life cycle management, data subject rights, data protection as well as data discovery and classification. This will enable data protection officers (DPO) to enhance compliance while minimizing penalties.

Ensuring consent for IT application and personal data

More than 80% of U.S. adults believe potential risks that they face because of data collection by companies outweigh the benefits[2]. Little surprise then that nearly 60% of non-compliance penalties are due to lack of consent, unlawful processing of personal data or mishandling of data subject rights (see Figure 2).

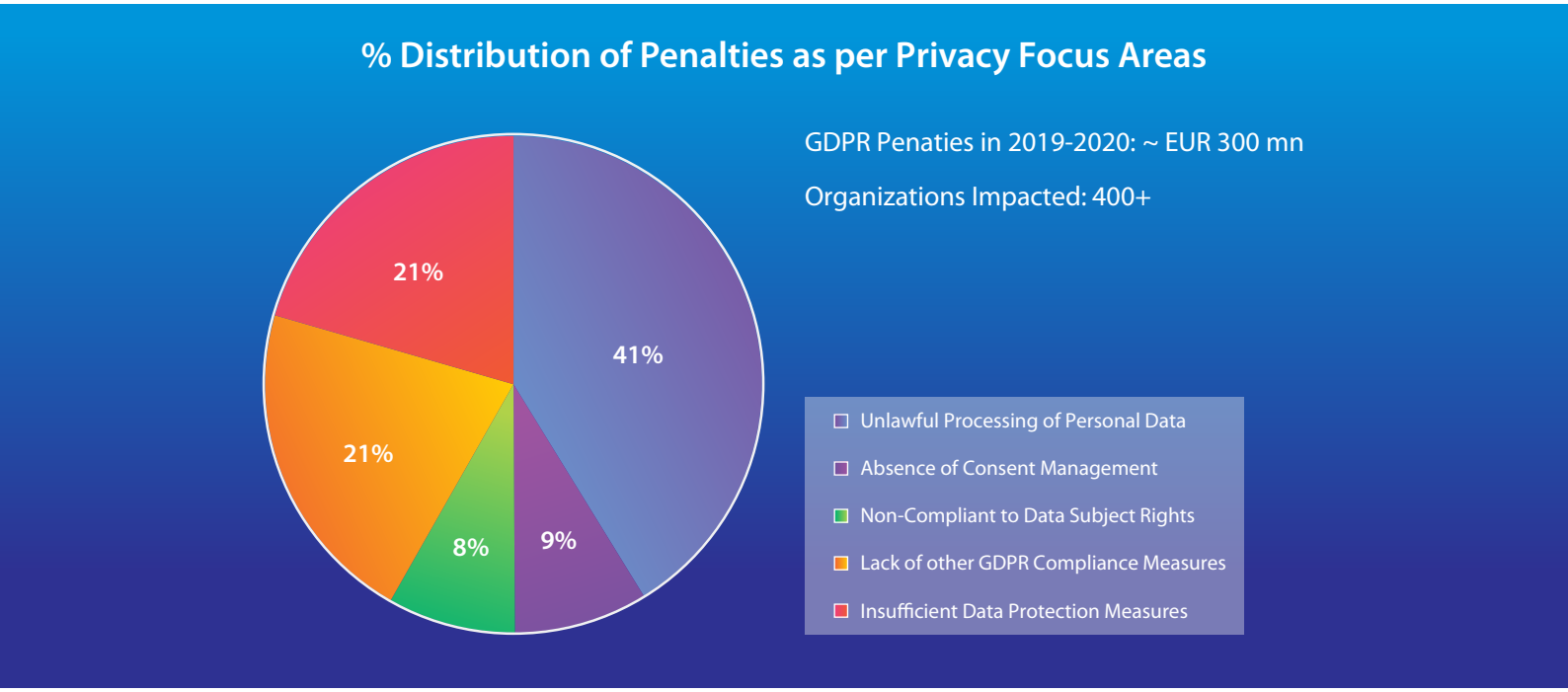

Figure 2: Penalties as per privacy focus areas

Automating consent life cycle management can help ensure consent for IT applications, employees and even vendors' personal data. This requires clearly defining the purpose of processing personal data, taking explicit consent for data collection by integrating consent solutions with front ends and ensuring enforcement of consent across IT applications based on real-time consent access.

In addition, the consent module features should also extend to websites for end-to-end cookie consent. Automated control over third-party cookies must ensure data is not collected until users or visitors consent to data collection from browsers. Dashboards for consent modules, too, can be made available to the DPO to provide a single-pane view of data processing in accordance with the consent provided. This can also be integrated with governance, risk and compliance tools to prepare consent maturity charts for the chief information security officer's (CISO) organization.

[2] *Pew Research Centre, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, November, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ , accessed January,21, 2021*

Improving response to data subject rights

For a large organization with about 5 to 10 million customers, the total unique personal data attributes about the customers that they can acquire could be over a 500 million. Ensuring data subject rights for even 1% of such a customer base within SLAs is time consuming, impacting employee productivity. Automation helps organizations rapidly respond to prominent data subject rights such as right to data access, right to data correction, right to data portability, right to delete and the right to stop sale of personal information with minimum manual dependency while ensuring accuracy and integrity of data. Integrating privacy tools with data stores that host personal data can help automatically generate response to data subject rights raised by any data subject or customer. This could reduce the time taken to handle data subject rights and manhours needed for manual handling of such requests.

Enabling data discovery and classification for revenue generation

As personal data becomes crucial for non-linear revenue generation, considering evolving data regulations and new laws in data processing internally, externally and through implementation of new applications are vital to enhancing compliance. This requires identifying types of personal data and leveraging artificial intelligence (AI) and machine learning (ML) to perform frequent scans in scheduled batches, discover patterns from structured and unstructured sources, classify discovered personal data as per policies and generate data lineage and data catalogs. The automated discovery of personal data and classification based on configured rules will reduce the need for manual workforce.

Boosting data protection

Integrating technology with existing cyber security or data protection tools can help protect consent-based data. For instance, access control based on classification can restrict access of certain user groups based on the classification assigned to files that contain personal data. At the same time, data can be masked dynamically at the database or file level for certain personal data attributes such as personal data on user interface (UI) screens. Similarly, de-identification of personal data can be achieved through the above methods for requests wherein an individual can exercise their right to be forgotten or erasure ensuring pseudonymization or encryption as required. Automating batch jobs can help archive or remove personal data from the IT enterprise based on the policies set for its retention, archival or secure purging.

Taking a structured and phased approach to build a privacy culture

While there is always a need for tactical fixes, a reactive approach may not effectively establish safeguards at all necessary checkpoints. Siloed approaches taken by individual business units would not provide a seamless experience to data subjects. Organizations need to develop an enterprise-wide mindset around data privacy which would direct all data privacy requirements to a centralized team who would directly report to the DPO or legal and compliance officer.

This centralized approach would highly benefit the organization during their external audits and compliance checks by regulatory authorities as all information would be available with a central team responsible for organization-wide data privacy policy and technology implementation.

Hence, organizations need to first assess their current data privacy posture and build a data privacy program encompassing all the privacy focus areas based on the assessment outcome (see Figure 3). This requires taking a structured and phased approach as follows:

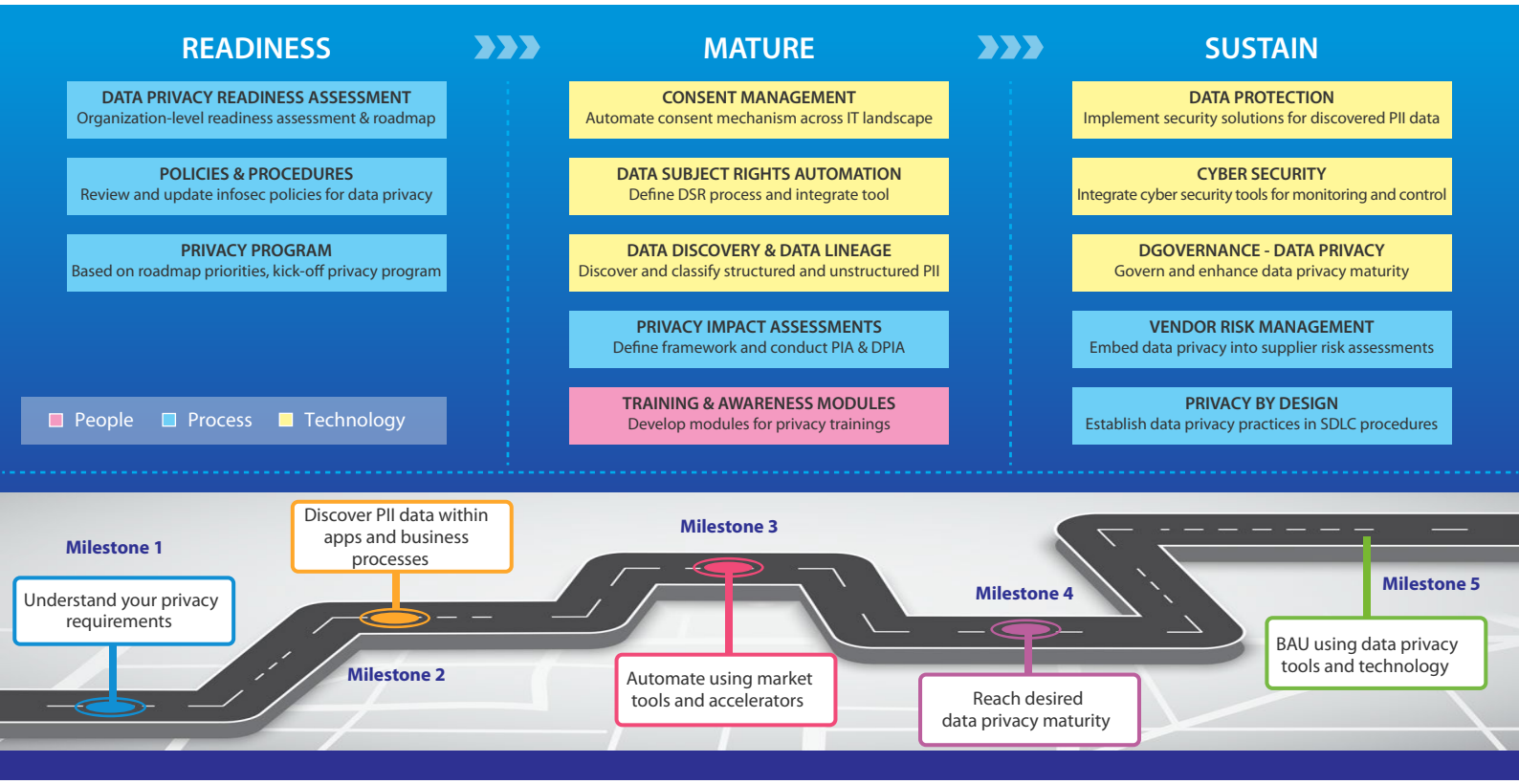

Figure 3: Taking a phased approach to data privacy

Phase I: Assessing data privacy maturity

Maturity assessment of the existing data privacy posture is crucial to evaluate business processes and personal data handling practices such as lawful processing, data collection and processing, consent management and data transfers. This helps determine key projects that can be executed under the data privacy program (see Figure 4.0). This enables organizations to build a detailed data privacy program plan, conduct time and effort analysis for each internal project and estimate cost of data privacy products and tools.

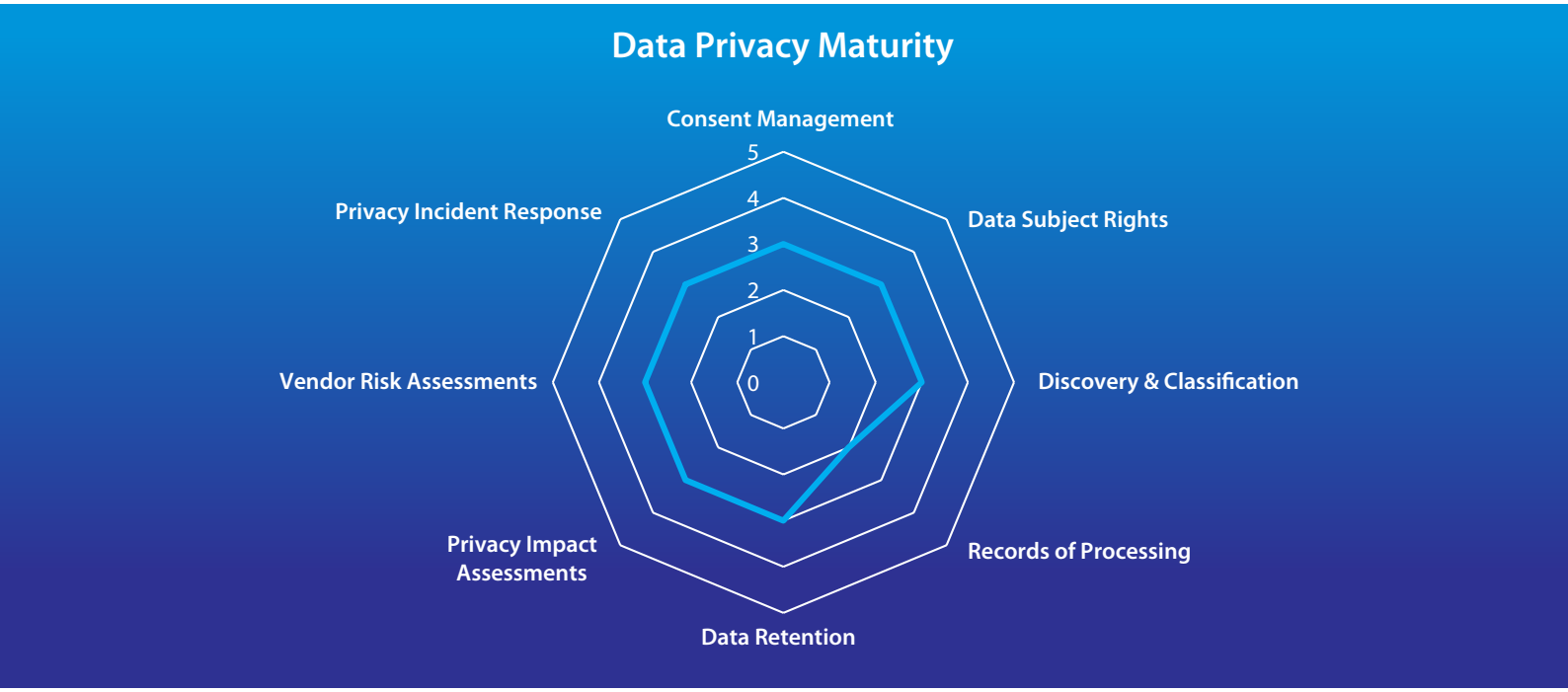

Figure 4: Data Privacy Maturity Chart

Phase II: Operationalizing data privacy program

Building a data privacy program requires analyzing each individual project and finalizing the tactical and strategic approaches to enhance the maturity of their data privacy posture. This helps focus on immediate quick wins and demonstrate efforts for privacy compliance to focus groups constituting of members primarily from the data privacy and compliance office. In addition, dedicated SMEs across privacy, legal, IT, human resources, business operations, corporate and administration departments can help process and handle personal data during their daily work processes.

Phase III: Automating data privacy

Operationalizing data privacy activities across business units and daily work activities requires successful implementation of data privacy tools. As company budgets focus more on their core services, investing in a heavy manpower-driven data privacy approach would not be feasible. Companies need a holistic, systematic, and automated approach to

manage immense complexities in providing consumers the autonomy on kind of data collected and its usage. These complexities will only grow as more consumers order products and services online, use more digitally enhanced products and services, and get post-purchase help through automated means.

As a part of the larger data privacy program, organizations need to identify areas that can benefit from automated data privacy tools, prepare the organization for deployment and ensure customized configuration of such products for sustainable data privacy automation initiatives, reducing the load on existing workforce and maintaining accuracy and integrity of data for future.

Unlocking growth with data privacy

With data privacy becoming a concern for consumers, ensuring safe handling of personal data is crucial to drive value from data and improve customer trust. A centralized data privacy program helps build a data privacy-oriented mindset and approach across the organization, including its people, processes and technology. This helps improve the organization's security posture, scale data privacy governance, integrate compliance policies in real time and build an audit trial, enabling organizations to keep up with the constantly evolving regulatory requirements around privacy policies.

About The Authors

Pratik Matkar

Lead, Data Privacy CoE, Cyber Security, TCS

Pratik currently leads the Centre of Excellence for Data Privacy within TCS' Cyber Security Practice. With over 16 years of experience in the IT sector, Matkar has led organization-level programs for business continuity and disaster recovery. He engages with TCS' clients, across various industry segments, to recommend customized approaches towards data privacy and protection programs.

Hussain Mirza

Lead – TCS Consent Management Solution, Cyber Security, TCS

With over 14 years of engagement in various roles within the information technology space, Hussain is the product owner of data privacy solutions in the Cyber Security Practice in TCS. With extensive consulting experience in data privacy, Mirza enables organizations to automate the most critical focus areas of data privacy including consent life cycle management and data subject rights.

Contact

Visit: Cyber Security page on https://www.tcs.com/

Email: cyber.security@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world's largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 469,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit **www.tcs.com** and follow TCS news **@TCS_News**.

Experience certainty. IT Services
Business Solutions
Consulting

Corporate Marketing | Design Services | M | 04 | 21