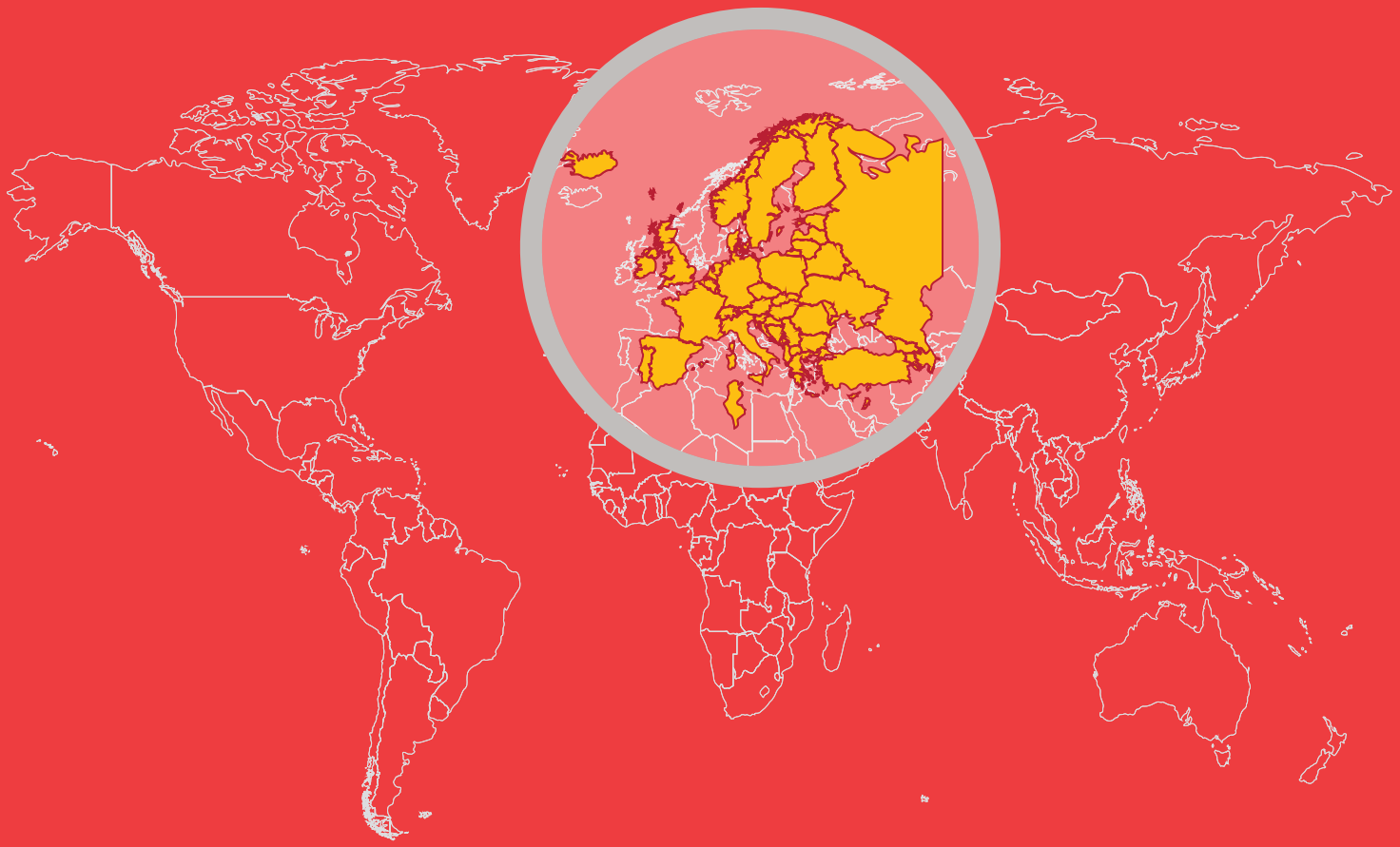
Demystifying the EU General Data Protection Regulation

pwc

www.pwc.in



On 25 May 2016, after a number of deliberations, the EU General Data Protection Regulation (Regulation (EU) 2016/679) was adopted. This development marks a milestone in the data protection laws across the EU region. The regulation will replace the current directive (EU 95/46/EC) by 25 May 2018, when it comes into full effect. Organisations have two years to understand, comprehend and implement the regulation in spirit and, as a consequence, demonstrate compliance.

The nucleus of the GDPR is to strengthen and unify data protection for individuals within the EU as well as address the export of personal data outside the EU. The core of GDPR is Personal data. Personal data means any information related to a natural person or 'data subject' that can be used to directly or indirectly identify the person. It can be anything from a name, photo, email address, bank details to posts on social networking websites, medical information, or a computer IP address.

It is important to understand what we mean by 'data'. The definition itself has changed significantly over time. Broadly, it can be divided into structured and unstructured data. Structured data refers to the basic details of a citizen, such as name, address and contact number. Structured data is consistent and resides in known and defined fields in the records. Unstructured data includes e-mails, videos, pictures, social media posts and anything which is not organised in a defined manner in a record. Organisations today collect both structured and unstructured data of customers, and at times, data that is not necessarily required for their specific business operations. Once the data has been collected, customers have little knowledge of and/or control over how that data is being used or shared.

In the recent past, there have been serious concerns over data leaks during high-profile breaches and incidents. As per estimates, there have been more than 575 reported data breaches which have exposed more than 13 million records in eight months in 2016. The data breaches span industries such as healthcare, telecom providers, cloud service providers, US federal agencies and large retailers. Some of the incidents that were reported in the last two months have actually occurred more than a year ago, but they were only detected by the organisations recently. Data protection has evolved as a concept over the years, but the issue of who controls and protects personal data has never been more critical.

The EU has always been at the forefront of designing and implementing programmes around data protection. The EU 95/46/ EC directive for data protection has been in practice for the past 21 years. However, the directive has been constantly challenged in terms of its applicability and adaptability to new age business (online services, smart devices, etc.). The digital ecosystem has changed the way people share personal information.

The GDPR is an essential step to strengthen and protect citizens' (data subjects) fundamental rights in the digital era. It gives data subjects access to clear and understandable information about their rights and where their data is processed. For businesses who have a global digital presence—both inside and outside the EU—the GDPR presents simplified and prescriptive guidance on mechanisms that need to be implemented to provide reasonable assurance to their customers on data protection.

1 1. Scope and Applicability

1.1 Data controller and data processor

An organisation that collects and processes personal data for its business transactions can fall under two broad categories—data controller and data processor.

Organizations work across the value chain to serve customers. Depending on the nature of work that is performed, they may fall under the category of data controller or data processor, or both.

An organization that collects personal data from the consumer and determines the purpose and the manner in which the personal data is to be used is a data controller. Personal data can be sent outside the boundaries of the controller for further processing. Organizations that merely store, collect and process data on behalf of a controller is a data processor.

A large IT services organisation which is headquartered in India but has sales offices in any country within the EU will be subjected to the GDPR. Another example is an Indian bank which has its data centre in India, but which has branches in the EU to serve both Indian nationals in the EU, as well as EU data subjects. Such a bank will come under the ambit of the GDPR.

An e-commerce website that is hosted and run from India but caters to EU data subjects will need to comply with the GDPR, even if the data is stored outside the EU.

1.2 Scope

The GDPR applies to any data controller or data processor which has EU 'establishments' where personal data is processed 'in the context of the activities' of such an establishment. Essentially, if an organisation has an office inside the EU and aims to target EU data subjects' personal data processing, the organisation, irrespective of whether it is a data controller or a data processor, will come under the ambit of the regulation.

The GDPR also applies to any data controller or data processor which does not have EU 'establishments' but which processes personal data of EU data subjects in connection with 'the offering of goods or services' or 'monitoring their behaviour'.

If the controller has establishments across different countries of the EU, it is the responsibility of the controller to identify a lead country and liaise with the authority in that country during the run-up to the implementation.

While the regulation specifically does not carve out applicability based on the size of business, an organisation must review its readiness to adopt the regulation and determine the scope and rigor of implementation.

1.3 Concept of processing

The idea of processing is very broad. It covers every processing operation that can be done on personal data, irrespective of whether it is undertaken by automated or non-automated means, or whether done actively or passively. The initial collection of personal data right through to its final deletion or destruction is considered processing, as are creating personal data, storing, using, copying, aggregating, adapting, amending, sharing, transmitting, archiving, selling, losing, and erasing the data.

The GDPR requires that controllers and processors of personal data shall act lawfully, fairly and transparently in their use of personal data and how they deal with the people to whom the data relate. Controllers have to be open and honest about what they are doing and why. They cannot, for example, mislead people about why they are using their data. Controllers have to stick to the purpose for which they acquired the data; minimise the amount of data held; and keep it accurate, up to date, and secure and confidential at all times. They must then delete or destroy it when the purpose for which the data was obtained or created is fulfilled, or if consent to use the data has been withdrawn. People who ask questions about what is happening with their data are entitled to answers and should be given copies of that data. If they have good grounds to ask for processing to stop, the request must be acknowledged and implemented.

The use of email to communicate is an example of processing of personal data. The generation of computer logs as we use our work systems or our personal devices also involves processing of personal data. Payment transactions when we shop on the high street or online also entail processing of data. The recording of CCTV footage and spoken word also involves data processing. Processing even occurs when we give feedback on our colleagues at appraisal time. Virtually every technology device and database that is used in a business processes personal data in some way.

2 Understanding the regulation: What's important?

The official journal of the EU GDPR has 99 articles across 11 chapters. A legal lens is needed to fully understand much of the regulation.

Although the regulation has undergone several important changes, the following five are the most important and impactful.

2.1 Data governance obligations

The governance layer is critical for controllers and processors to be able to plan and visualise an effective data protection programme. The regulation recognises this and is therefore prescriptive about a range of measures that organisations need to adopt to take data protection seriously.

Data minimisation and pseudonymisation: The GDPR does not apply to any data that does not relate to an identified or identifiable person. If data is anonymised in a manner that the data subject is unidentifiable, then the GDPR does not apply to such processes. In reality, it may not be possible to completely anonymise data and continue to meet the objectives of processing. This brings the concept of pseudonymisation into the picture. Pseudonymisation is the separation of data from any direct identifiers and linkages to the data subject while maintaining the utility of data. The regulation outlines incentives for organisations who pseudonymise data, because it significantly reduces the risks of a potential leakage that could cause harm to the subjects. Also, the regulation relaxes controls around the unlawful processing of pseudonymised data with the consent of the subject.

Privacy by design: Organisations must implement controls—technical and procedural—that are tightly integrated with the data processing activities. The word 'design' refers to the adoption of privacy and protection mechanisms while designing a processing activity. Organisations that already perform processing of personal data need to be able to trace back to the basics of data collection, retrofit protection controls, redesign the process where applicable and demonstrate continuous compliance.

Standard methods of encryption pose adoption issues for large-scale personal data processing, due to performance as well as cost issues. Encryption also alters the data structure of the stored information and therefore requires significant re-architecture of technology systems. But it is a powerful concept when applied selectively. Organisations should focus on separating the metadata from the actual data. This removes the linkage to a directly identifiable data subject. With no direct identifier, the GDPR now applies to a limited set of the metadata which mostly contains personal information. Encryption techniques could be adopted on the metadata, with the keys being available to a set of select data owners, thereby reducing the threat surface area.

Privacy impact assessments: A privacy impact assessment is an effective mechanism to determine why personal data is being collected and how the data that is collected is being used, accessed, processed, safeguarded and stored. It also helps in identifying the risks and effects of keeping personal data and in evaluating protection mechanisms to mitigate the risks. Much like security risk assessments, a privacy impact assessment is performed prior to onboarding/acquiring a new programme that stores, accesses and processes personal data; inducting any technology that handles personal data; and implementing any significant changes in the processing logic. The impact assessment frameworks that organisations use must be repeatable and scalable.

Some Indian organisations who already have a data protection programme use various privacy frameworks. Such frameworks also have a tool for privacy impact assessments. The framework and impact assessments are largely based on industry best practices. With the GDPR, the focus must now shift towards three areas—viz. adopting the prescriptive nature of controls in the regulation across several areas, enhancing the existing framework to reflect the requirements of the regulation and relooking the scope of processing in the context of the regulation.

2.2 Data subject rights

This is probably one of the most important changes that has been outlined in the GDPR compared to the EU directive.

Data subjects have the right to have their data 'erased' (or forgotten) in some circumstances—essentially when the processing does not satisfy the requirements of the regulation or when data is unlawfully processed. Unlawful processing could refer to something as basic as the absence of a valid purpose for the collection or processing of data, or the processing of information without justification and explicit consent from the data subject. When a data subject notifies the intention to exercise his/her rights, the controllers are bound to respond without any unnecessary delay (i.e. within 30 days).

Having a current and updated map of all the systems which store or process personal data is critical. Among other things, this shall aid organisations in being agile to implement data erasure requests from data subjects. Building a map of systems is quite a complex exercise, especially when organisations have interconnected systems and data flow is seldom captured as a part of the design. Further, if there are changes that need to be made to reduce the scope of regulation that applies to the controller, surgical analysis needs to be done to understand the impact of technology changes, application behaviour and database schemas—which may call for re-architecting the overall technology stack in certain cases.

This poses several challenges for controllers.

- Firstly, the controller needs to have a clear understanding of where personal data is stored and processed in the organisation. While the collection point may be a single system, activities related to processing could lead to data traversing several systems.
- Secondly, controllers may have shared data with their partners for processing. Even if we assume that explicit consent was sought by the controller from the data subject for the sharing of personal data with the partner ecosystem, the power balance now tilts towards the data subject. If the data subject decides to port out of the controller and therefore requests erasure, the controller now needs to inform and get the erasure implemented across all the partners with whom the data has been shared.
- Thirdly, from a technology standpoint, erasure is not as simple as it seems. It goes beyond simple file deletion which just removes pointers to the base data sectors. This data can be easily recovered using basic software. Organisations must carefully evaluate technologies which suit their infrastructure ecosystem in order to be able to effectively demonstrate compliance to this regulation.

Another significant change that is a part of the GDPR is the concept of data portability. Data subjects will have the right to transfer their personal data in the commonly used electronic format from one data controller to another without any hindrance from the original controller. Organisations need to think about building an ecosystem that enables them to make data portable, with costs and efforts being commensurate with the risk of non-compliance.

2.3 Better quality of consent

Article 4(11) of the GDPR defines 'the consent of the data subject' as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

The focus is on 'unambiguous', which means that consent needs to be explicitly obtained through affirmative action from the data subject to justify the processing of personal data.

Over the years, controllers and processors accumulate personal data of data subjects that has been collected through implicit/opt-out consent. This aggregation of data results in the development of several use cases for data mining and analytics, which helps organisations to profile customers and thereby serve them with personalised offers. However, the new regulation on the requirement of explicit consent for such kind of processing, if it entails non-pseudonymised data, may disrupt such uses of data.

Additionally, controllers need to relook all the data collection points (physical forms, online website questionnaire, security cookies, etc.) to ensure that adequate explicit consent is being sought along with reasons.

Selecting a particular option by ticking a box on a website, choosing certain settings or explicitly accepting certain terms and conditions are examples where the data subject clearly indicates the proposed processing of personal data. Any opt-out settings, such as pre-ticked boxes, shall not be acceptable.

2.4 Breach notifications

Organisations will be required to report serious contraventions of the law to the regulators and subjects affected within 72 hours of becoming aware of a breach.

Broadly, there are three aspects to addressing this:

- Organisations must be able to detect a breach. This would require organisations to have a full view of the personal data they store and/or process, effective collection mechanisms of both application and operation system logs of the sub-systems, and fine-tuned use cases that are contextual. Breach indicators must be developed and standardised to address known threats. Merely having the best of frameworks, tools and technologies do not yield any value when it comes to detecting a breach within acceptable limits. The core constituent of a sound breach detection programme is skilled resources who are able to observe the indicators and conclude on suspicious activities without raising false alarms.
- Once a breach has been detected, the response programme is critical for containing the extent of damage. An effective response team needs to have diverse skill sets across networks, applications, data protection technologies and operating systems, and should be able to work cohesively to contain the effects of a breach. Several organisations outsource the breach response programme to experts. In such cases, they must carefully agree on service levels with the expert team for agility of response.
- Historically, a large number of data breaches have occurred due to a lack of adequate controls with vendors of organisations with whom personal data is exchanged to support the processing objective. The controller organisation is eventually held accountable for the breach, although it has little control over the vendor's breach detection and response programme. In such cases, the application of data minimisation techniques is a must in order to pseudonymise data that results in no significant impact in the event of a breach.

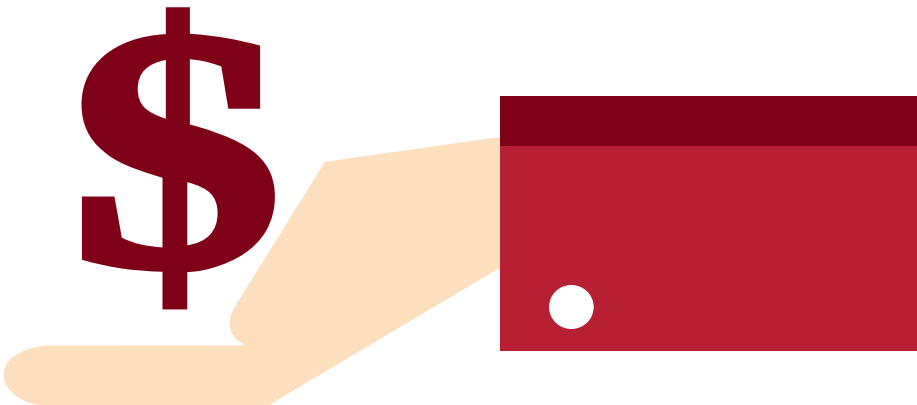
2.5 Fines

The GDPR has outlined a tiered approach for penalties for a breach which applies to both data controllers and data processors.

- Obligations-related non-compliance could result in a penalty of 2% of the annual turnover or 10 million EUR, whichever is higher, in case of less serious violations.
- In case of serious violations such as non-compliance to certain basic principles of the regulation, like consent or rights of the subject to approved mechanisms of data transfer, the fines could be 4% of the annual global turnover or up to 20 million EUR, whichever is higher.

Fines could be levied when there is a data breach that did not get reported within the stipulated time frame or when the data protection authorities detect a non-compliance during their checks. Organisations must therefore ensure that they focus on ensuring compliance to the regulation at all times, starting with high-risk, high-impact processing operations. In the next two years, the cost of compliance and implementing the regulation may seem like an expensive proposition for controllers and processors. However, organisations must be prudent in taking decisions to invest appropriately now in order to avoid long-term negative cash-flow implications.

Technology and business process outsourcing companies who process personal data for clients who service EU data subjects must relook their liability clauses in client agreements and structure them appropriately. Controllers and processors must also have contingency plans in terms of insurance agreements in place in case of unforeseen events.



3 Approach to get started

Approach to get started

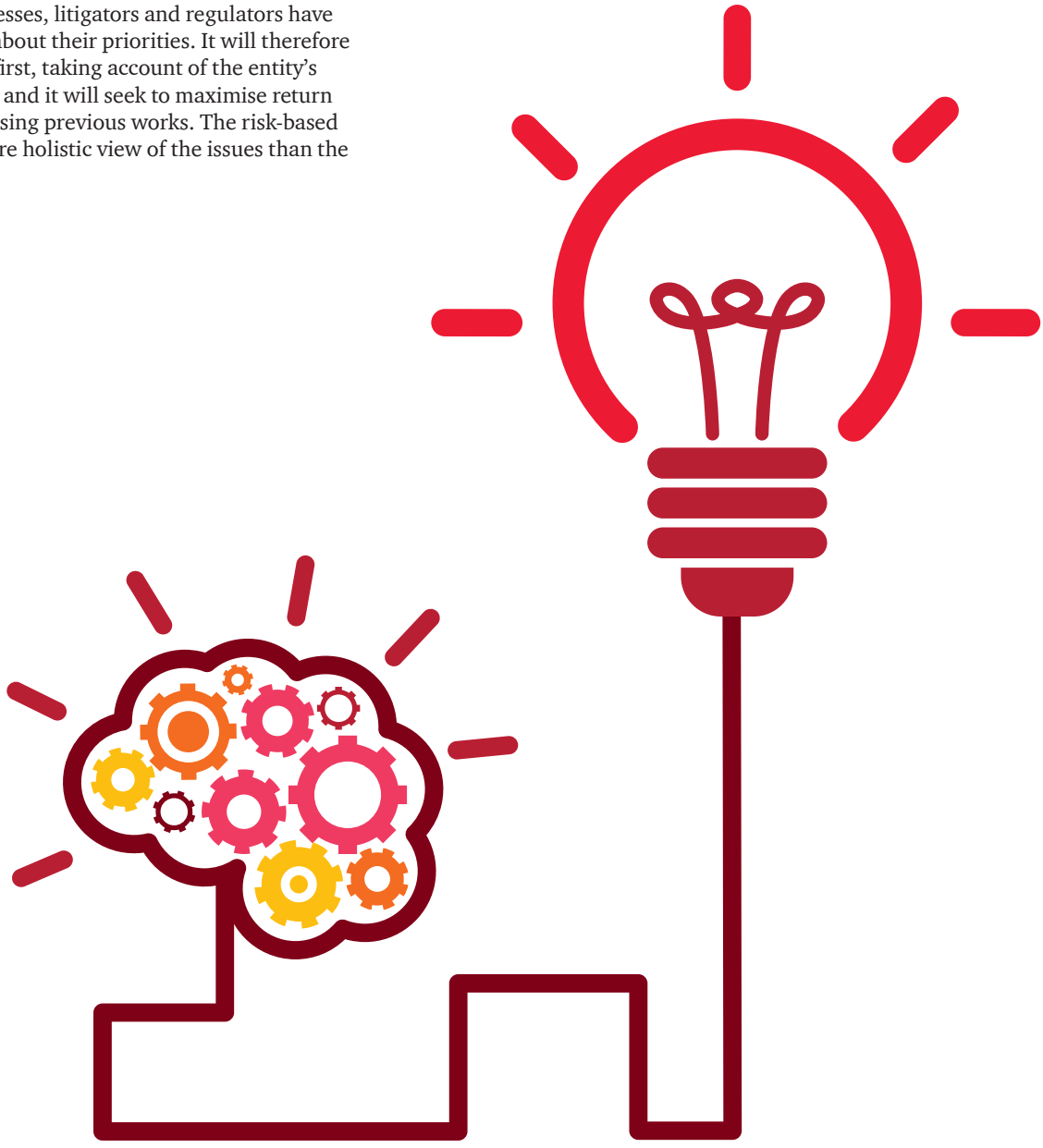
The GDPR raises countless compliance issues. It will be very easy to get lost. Work needs to be prioritised so that critical processing and risk issues are addressed before matters of less importance.

There are two distinct approaches to adopting and implementing the regulation:

- Legalistic/compliance-based approach: The legalistic approach to GDPR compliance focuses simply on the legislative requirements within the GDPR, without any weighting for risk or the organisation's key business objectives. Generally speaking, the legalistic approach will deliver the same compliance programme shape for all entities.
- Value protection-based approach: This approach is risk based. It recognises the operational realities of an organisation's processing or business activities and the way the law is enforced in practice. The risk-based approach recognises that, in the real world, businesses, litigators and regulators have to make tough choices about their priorities. It will therefore tackle major risk areas first, taking account of the entity's key business objectives, and it will seek to maximise return on investment by reutilising previous works. The risk-based approach requires a more holistic view of the issues than the legalistic approach.

Optimum programme design begins with the statement of a vision for the entity's desired end state. The vision is the articulation of the entity's aims and objectives, which provides an ongoing reference point for the work over time, to ensure that the business priorities are kept at the forefront. The strategy for the compliance programme has to be fully aligned with the vision. Once the strategy has been developed, the entity can establish the structures that are necessary to support the vision. Many entities rush to begin work on structures rather than spending sufficient time considering the vision and strategy. This is a key problem of the legalistic approach.

Irrespective of the approach adopted by organizations, a good starting point in this journey is to perform a self-assessment as per the requirements of the regulation. The assessment must result in a clear understanding of the scope of the implementation of the regulation as well as the extent of process and technology changes that one needs to adopt to comply with the regulation.



Notes

Notes

Contacts

Sivarama Krishnan
Leader, Cyber Security
Tel: +91 (124) 626 6707
Email: sivarama.krishnan@in.pwc.com

Siddharth Vishwanath
Partner, Cyber Security
Tel: +91 (22) 6669 1559
Email: siddharth.vishwanath@in.pwc.com

Manu Dwivedi
Partner, Cyber Security
Tel: +91 (0) 80 4079 7027
Email: manu.dwivedi@in.pwc.com

Sundareshwar Krishnamurthy
Partner, Cyber Security
Tel: +91 (22) 6119 8171
Email: sundareshwar.krishnamurthy@in.pwc.com

Hemant Arora
Executive Director, Cyber Security
Tel: +91 (124) 626 6717
Email: hemant.arora@in.pwc.com

PVS Murthy
Executive Director, Cyber Security
Tel: +91 (22) 6669 1214
Email: pvs.murthy@in.pwc.com

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

pwc.in

PD/September2016-7381