



EU General Data Protection Regulation (GDPR)

Point of View for ERP and HRMS
Operations

For private circulation only

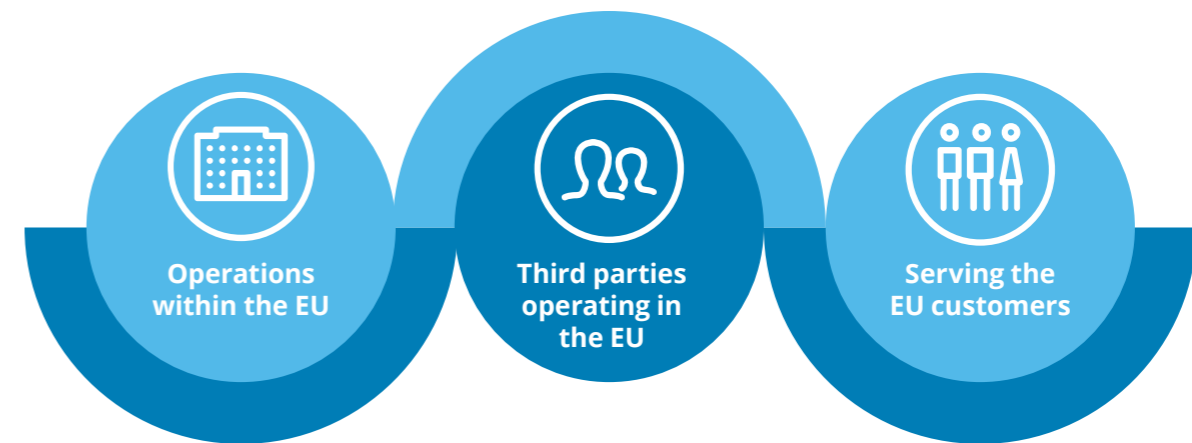
Risk Advisory



Preface

Does the EU GDPR impact organisations in India?

Yes! This new law will have a profound impact on the operational and control environment of the organisations, not only within EU but also within the organisations based outside the EU having:



This is a border less and sector neutral legislation. It goes beyond EU to 'organisations offering goods or services to customers in EU', 'organisations that monitor the (online) behavior of the EU customers' and during these services such organisations access/process/host/store "personal data" of EU customers.

With enforcement date approaching fast (25 May 2018), organisations are recommended to quickly assess GDPR's applicability and initiate readiness journey at the earliest.

Note: Map on this slide is only for the representation purposes.





Content

Understanding this new regulation	6
Key considerations for ERP environment	11
Are you prepared?	12
How can we help?	13
Key contacts	14

Understanding this new regulation

How it applies to Indian organisations?

- The General Data Protection Regulation (GDPR) is a law or a regulation which was adopted by the European Commission on 27 April 2016.
- It is scheduled to go into enforcement effective 25 May 2018 and is expected to impact organisations across the globe that do business in Europe.
- A core feature of the GDPR is that as a regulation, rather than a directive, it does not require enabling legislation in each member state, something that historically led to inconsistencies.
- As per the Article 2 "Material Scope", this regulation applies to the processing of personal data wholly or partly by automated means.
- Applicability (as per the Article 3 "Territorial effect") of GDPR is linked to the processing of the "personal data"
 - In the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not.
 - Of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services, to such data subjects in the EU; or the monitoring of their behaviour as long as their behaviour takes place within the EU.
 - By a controller not established in the EU, but in a place where member state law applies by virtue of public international law.

Is it a 'must' to comply?

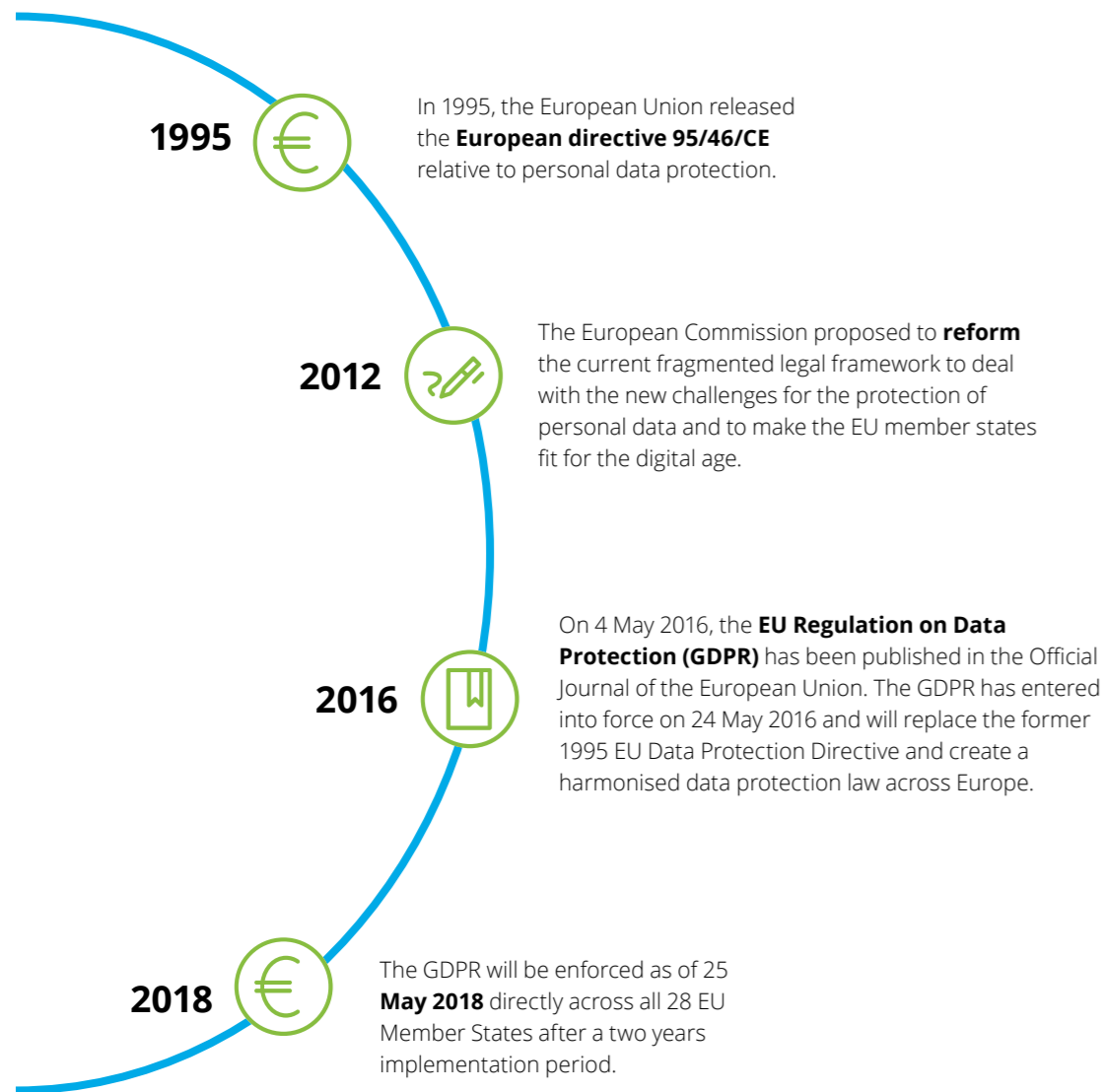
Yes, if your organisation is subject to this regulation.

Any impact of its non-compliance?

Key impact – penalty of maximum 4% of annual worldwide turnover or €20 million (greater of the two)!!!

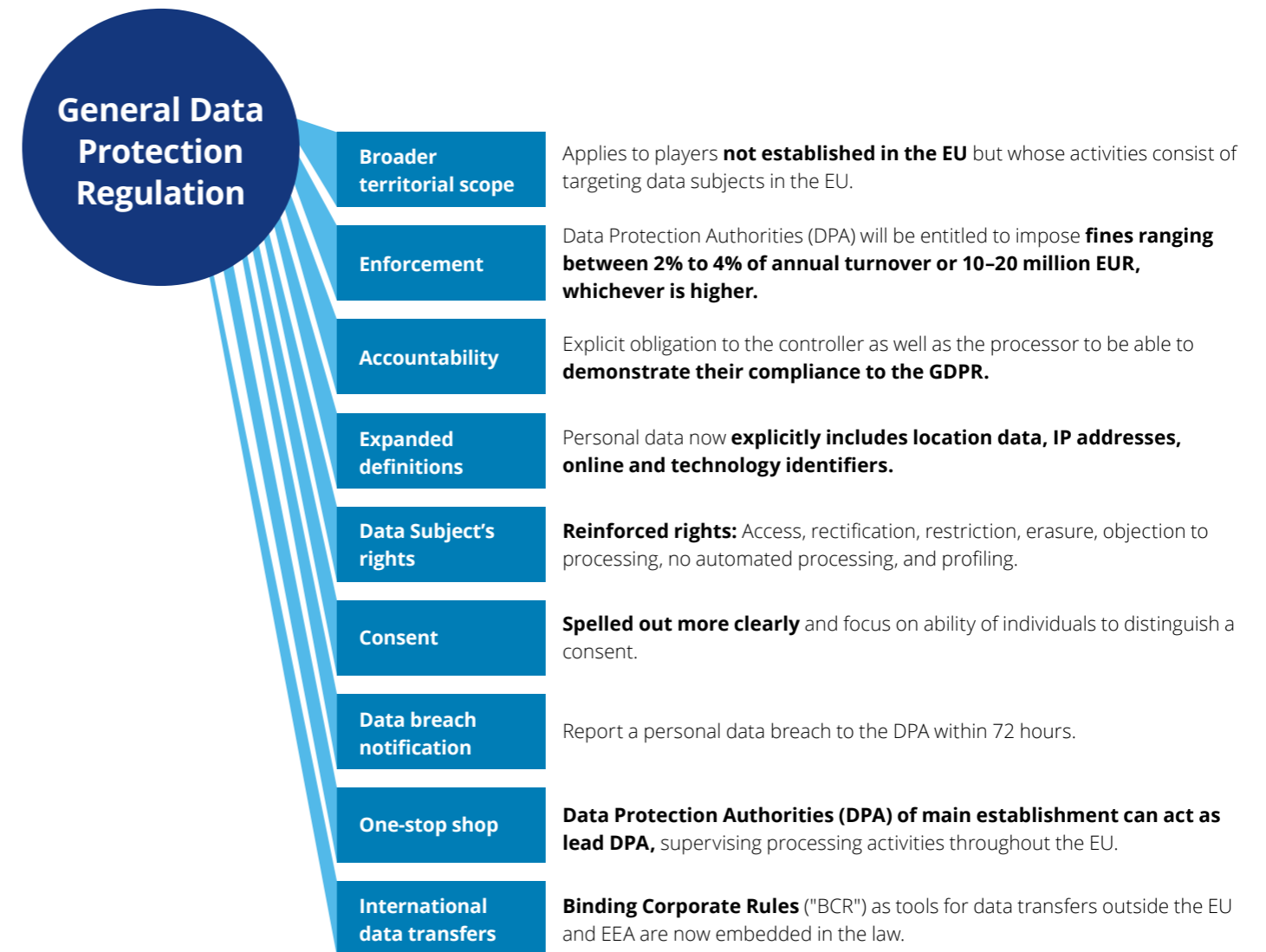


How it evolved?

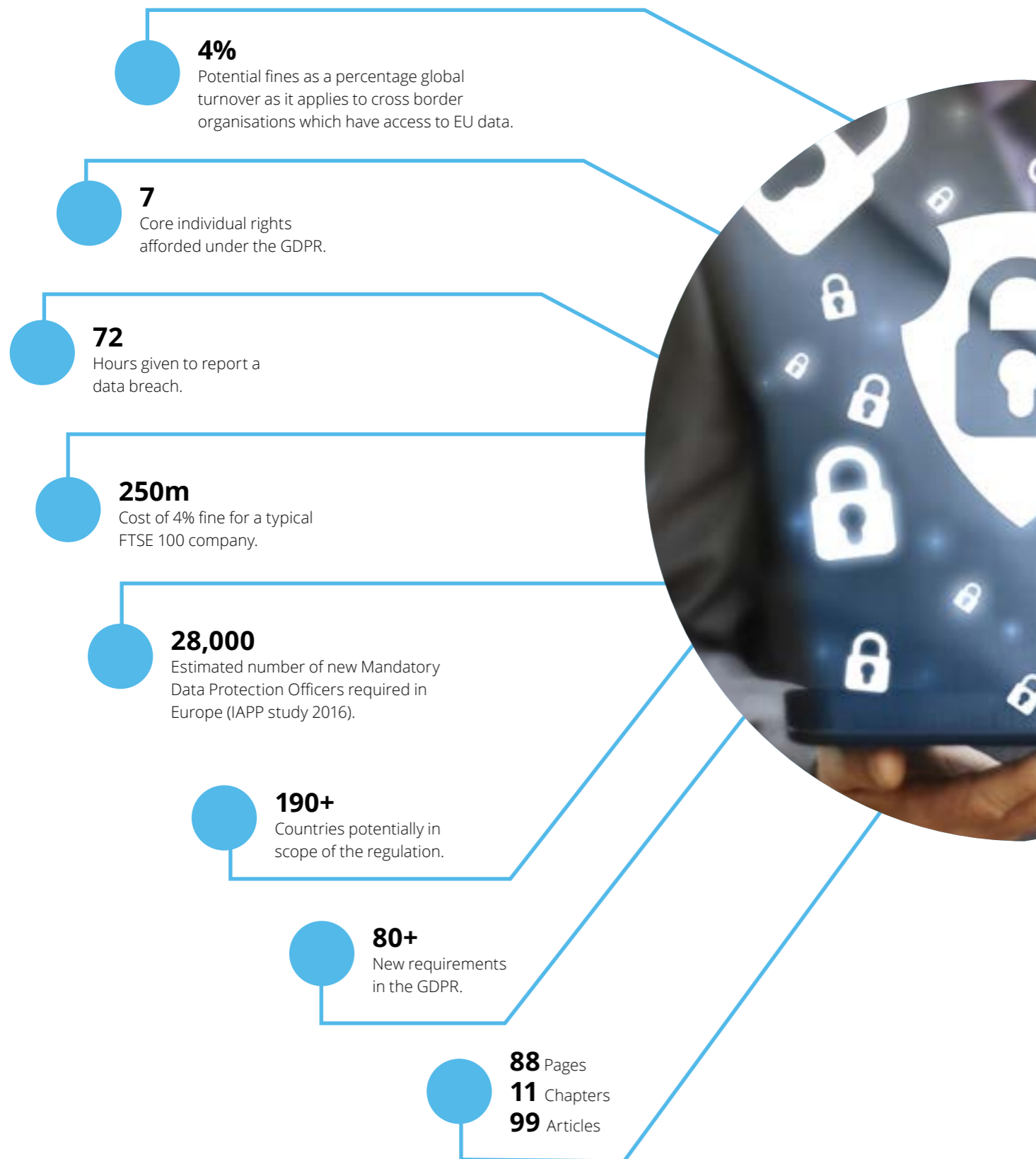


What has changed?

What has changed from the former 1995 EU Data Protection Directive?



Understanding GDPR in numbers



Key considerations for ERP environment

Organisations today use various ERP solutions while dealing with their business partners (e.g., employees, customers, vendors etc.) and many capture personal data of these data subjects. It is essential to understand which of these data subjects and personal information is covered under GDPR (as briefed in preceding section). ERP also emphasises on ease of user experience and have been aggressively pushing solutions like mobility, cloud, etc., which adds newer dimension to data access. Holistic view is required where ERP and non-ERP applications co-exist while performing the impact assessment.

- ERP solution facing retail customers e.g., IS Utilities, IS Retail or any other similar solution capturing information of retail customers which can be treated as sensitive information under GDPR.

- Employee information can be captured using ERPs like SAP HR, SAP Success Factors, SAP ESS/MSS, etc.
- Creation of employees as vendors for advances, expenses in ERPs like SAP HR, SAP FICO, concur, etc.
- Organisations may also go for a hybrid approach where employee data is shared across ERP and other applications using interface/data exchange



- Covered persons under GDPR are individuals (may be employees, consultants, vendors, etc.) or customers in EU. Their personal data gets recorded in ERP applications such as (SAP MM module/SRM tools, e.g., Ariba, etc.)

- Customer information including client and contact details of key client contact person may become a sensitive information under GDPR.

- Analytical tools extracting data from ERP may replicate sensitive information for employees, and customers or a combination of multiple applications, such information may be sensitive under GDPR.

ERP environment is accessed by various departments, functions within organisation and ERP support by vendors. While evaluating GDPR impact around ERP operations it is recommended to consider data residing in non productions instances like development, quality and test. Data exposed using interfaces and mobile application utilities will necessitate the need for tools to perform data masking, data archival and data encryption.

Are you prepared?



Respond

- Do you have a process to enable data subjects' rights such as request for access/ portability or erasure?
- Is there adequate processes in place to respond and notify data breaches?



Governance

- Are roles and responsibilities defined?
- Has an assessment of the organizations' risk exposure from EU GDPR been conducted?
- Do you have oversight of the data lifecycle from the point of origin to destruction?
- Is there a process for identifying and responding to local regulatory requirements in addition to GDPR?



Monitor

- Are compliance metrics identified and measured?
- Are processes, systems, and networks monitored to identify data access, use, change and breaches?



Assess

- What types of data do you collect, and where does the data originate?
- Are adequate controls in place for use, processing, storage, transfer and destruction?
- Are Privacy Impact Assessments conducted as required?
- Are internal and independent reviews conducted on a periodic basis?



Protect

- Do you have a process to perform a risk analysis or new or changing business processes?
- Is Privacy by Design and Privacy by Default incorporated within the processes?
- Will you able to erase data when requested?
- Are technological safeguards in place to protect sensitive data?

How can we help?

Our service offerings*

Deloitte has a dedicated team of specialists with a deep expertise in privacy data protection programs across large scale and complex organizations, embedding change and offering a full spectrum of **GDPR related services**:

 GDPR readiness assessment	 Change programme design and delivery	 Third party management
 GDPR compliance roadmap	 Incident Management Framework	 GDPR program monitoring and roll-out strategy
 Global privacy compliance assessment	 Data discovery, mapping, and inventories	 Governance and compliance review
 GDPR technology impact assessment	 Privacy-by-design advice and application	 Privacy risk and compliance training
 Privacy programme development	 Data leakage protection	
 Privacy strategy and roadmap development	 Privacy impact assessment and health check	

*Deloitte Touche Tohmatsu India LLP offers advisory services on aspects related to Governance, People, Technology and Processes to help address the requirements under GDPR. Kindly note that Deloitte Touche Tohmatsu India LLP does not provide any legal advice, including any legal advice relating to privacy or data protection laws.

Key contacts

National

Amry Junaideen

President - Risk Advisory
amjunaideen@deloitte.com

Shree Parthasarathy

Leader - Cyber Risk
sparthasarathy@deloitte.com

Regional

Mumbai

A.K. Viswanathan

Partner - Risk Advisory
akviswanathan@deloitte.com

Abhijit Katkar

Partner - Risk Advisory
akatkar@deloitte.com

Vishal Jain

Partner - Risk Advisory
jainvishal@deloitte.com

Priti Ray

Partner - Risk Advisory
priray@deloitte.com

Munjal Kamdar

Partner - Risk Advisory
mkamdar@deloitte.com

Bengaluru

Maninder Bharadwaj

Partner - Risk Advisory
manbharadwaj@deloitte.com

Gaurav Shukla

Partner - Risk Advisory
shuklagaurav@deloitte.com

Praveen Sasidharan

Partner - Risk Advisory
psasidharan@deloitte.com

Delhi

Gautam Kapoor

Partner - Risk Advisory
gkapoor@deloitte.com

Hyderabad

Ramu Narsapuram

Partner - Risk Advisory
ramun@deloitte.com

Pune

Ashish Sharma

Partner - Risk Advisory
sashish@deloitte.com



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.