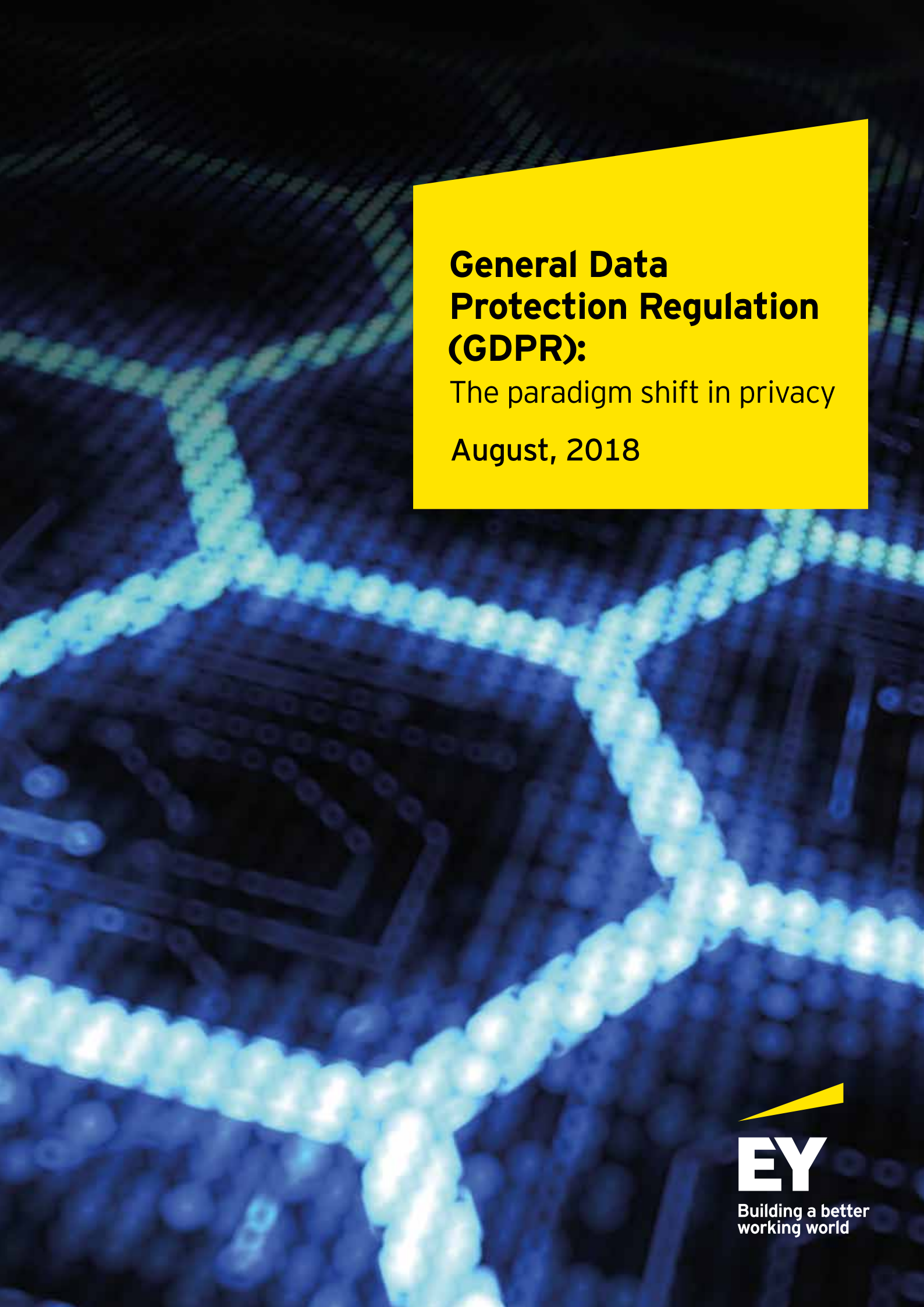


General Data Protection Regulation (GDPR):

The paradigm shift in privacy

August, 2018

EY
Building a better working world

Content

Foreword

The General Data Protection Regulation (GDPR) is the most significant law introduced in the European Union's history, the resultant of rigorous discussions about the privacy arrangements and numerous amendments of previous directives. The successor of 1995 Data Protection Directive, GDPR gives good room for varied interpretations and implementations to meet its requirement. Despite these liberties, GDPR is stringent in terms of meeting its specific requirements, like trans-border scope, privacy by design and default, in addition to numerous others. GDPR also sets expectations and benchmarks for developing privacy laws and regulations across the world.

It is imperative to identify the influence of GDPR and prepare for upcoming orientation of world which will be focused on data privacy, protecting rights of the people and security of their data. The path to ensure GDPR compliance has not been easy for organisations. The scope of varied interpretations and uncertainty in surety of the implementation steps to be undertaken has left a lot of organisations across industry sectors baffled.

As organizations continue to work towards GDPR compliance, India moved closer to its first data privacy law on Friday, 27th July, 2018 after a committee, headed by former Supreme Court judge BN Srikrishna, proposed a draft Personal Data Protection Bill. With growing concerns around data privacy in an increasingly digitising economy, it will be interesting to see how Indian organizations cope up and respond to the upcoming regulation. Those who have initiated their journey towards ensuring GDPR compliance would definitely have an advantage over the ones who are yet to align their business goals with privacy principles.

This report is based on a survey conducted by EY to assess the status of India's current levels of GDPR compliance and the results showcase India Inc.'s journey while highlighting the advantages, setbacks and the challenges they have faced so far. EY acknowledges and applauds the respondents who took out their valuable time to participate in the survey and we do hope you find the report insightful.

We believe the outcome of this report will set the tone for our various stakeholders across the country and would give a fresh perspective about the approach being undertaken in the industry towards data privacy.

Jaspreet Singh,
Partner – Cyber Security, EY

Vidur Gupta,
Partner – Cyber Security, EY

1 The onset of General Data Protection Regulation (GDPR)

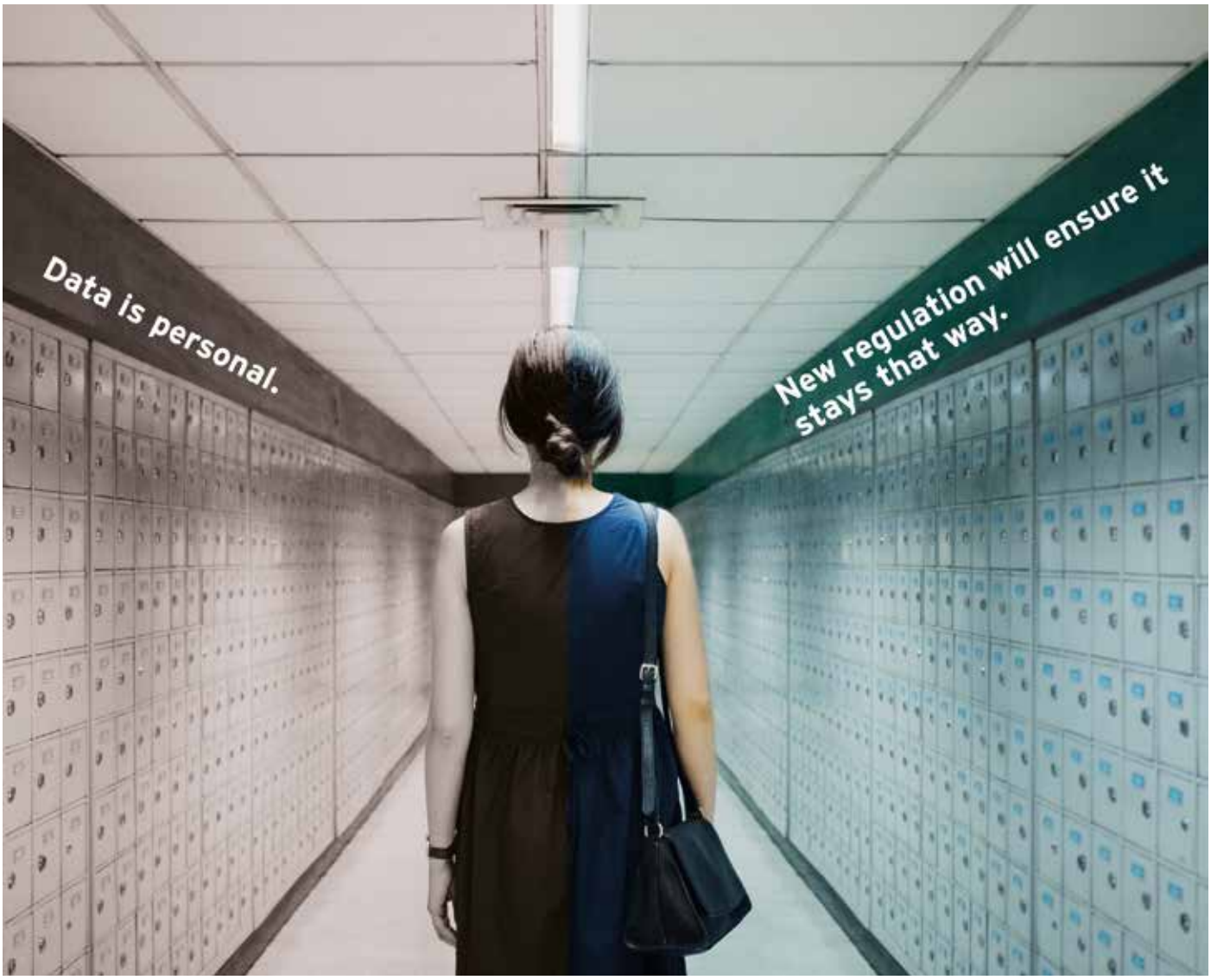
The beginning of a paradigm shift in the global data privacy landscape with European Union's GDPR:

Privacy has been a major area of concern in the past, continues to be in the present and may remain so in the future. As digital disruption continues to challenge privacy norms across the world, cloud, social media and mobile technology advancement is fundamentally altering the personal and professional lives of people across the globe. The constantly changing threat landscape driven by the connected world is forcing law enforcement agencies to enhance the privacy legislation regime regularly. Today, this is one of the biggest challenges encountered by many organizations as they grapple with the introduction of newer legislations and frameworks around data privacy. The concerns around data privacy impact both consumers and enterprises alike. While consumers are concerned about the misuse of personal and sensitive information, organizations are worried about having a dampening impact on their reputation, brand value, consumer trust as well as revenues. With the GDPR coming into force from 25 May 2018, organizations will need to evaluate where they stand in their data privacy journey as the onus of accountability shifts from regulators to organizations. Organizations need to understand and document what data is acquired, maintained and processed, and the legal basis for it.

With GDPR, EU residents have gained more control over their personal data as organizations will be held responsible for the data they process and they will also have to obtain explicit consent from the residents to process it.

With two months of coming into effect, GDPR compliance is still one of the key focus areas for organizations across the globe. As per the reports*, there has been a **50% increase** in the number of complaints since the legislation came into effect as compared to the corresponding period last year.

With a large number of organizations providing goods or services, or monitoring behaviour of consumers in the EU, India Inc. cannot be left behind in its GDPR compliance journey.



** https://www.theguardian.com/technology/2018/jun/26/european-regulators-report-sharp-rise-in-complaints-after-gdpr*

2 Key changes introduced under the GDPR

What you need to know to stay compliant?

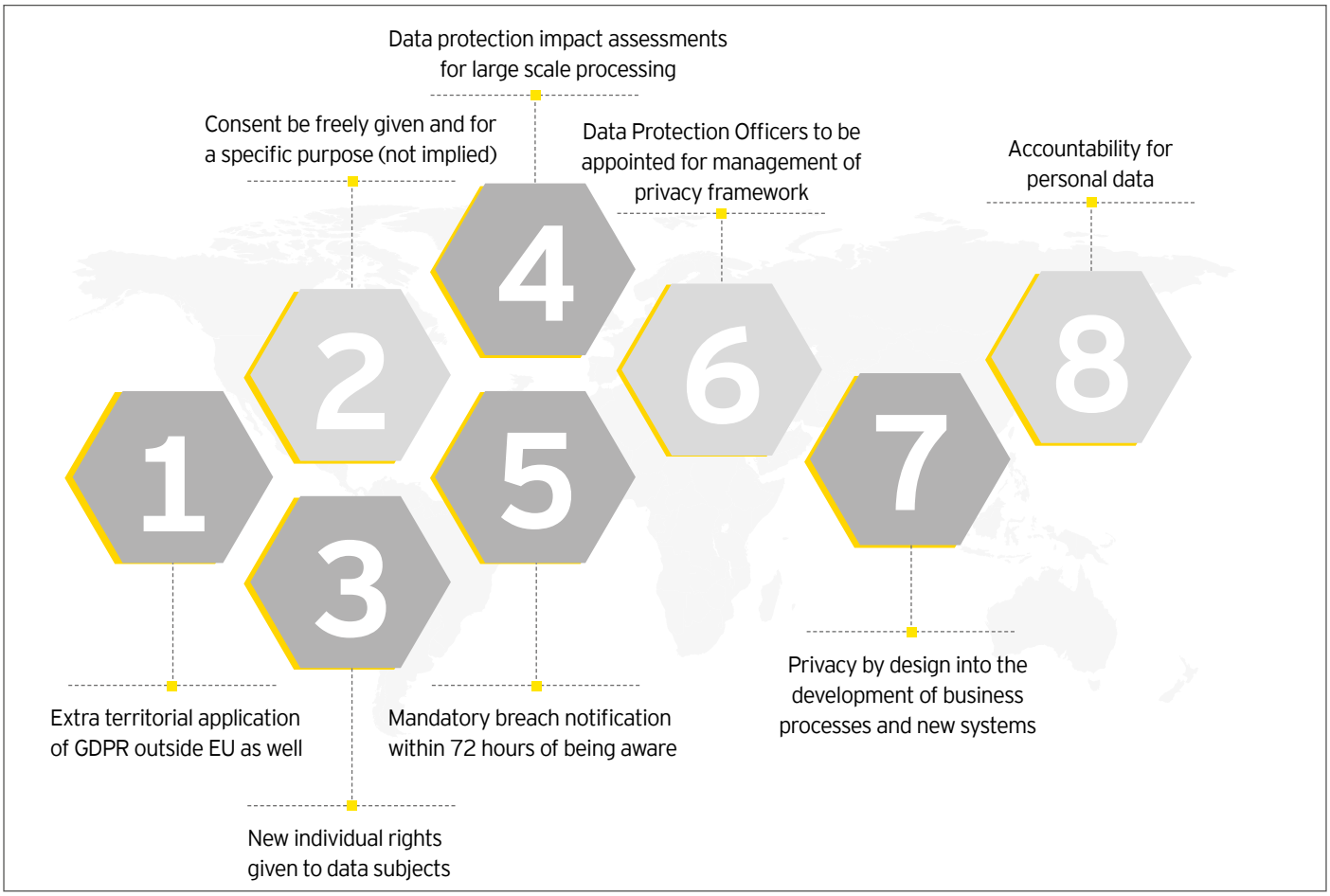


Figure: Key changes introduced by GDPR

Global Implications of GDPR

- Applies to all data controllers and processors established in the European Union (EU) and organizations that target the EU citizens outside of the EU.
- Fines for a breach of GDPR are substantial. Regulators can impose fines of up to 4% of total annual worldwide turnover or €20,000,000, whichever is greater.
- GDPR us applicable to all organizations that have an establishment in the EU, provide goods and services to EU citizens or monitor behaviour of customers based in the EU

Source: EUGDPR.org

Acquiring explicit consent

- Consent must be 'explicit' in case of sensitive personal data or trans-border dataflow.
- Customer consent to process data must be explicitly obtained and for specific purposes
- Customers must be informed abouttheir right to withdraw consent

Enhanced and new data subject rights

- GDPR is a landmark development in the global privacy landscape as it has introduced,
  - The right to be forgotten – where individuals have the right to ask data controllers to erase all personal data without causing undue delay under any circumstances
  - The right to data portability – where individuals can request service providers or data controllers to 'port' their data to another provider, provided it is technically feasible.
  - The right to object to profiling – the right to decline being subjected to a decision solely based on automated processing.

Data Protection Impact Assessments (DPIA)

- Organizations must undertake DPIA when conducting risky or large-scale processing of personal data. The DPIA shall be conducted mandatorily every three years.

Privacy by Design

- GDPR focused to embed privacy into the culture of the organization and therefore any activity that an organization undertakes shall be assessed for its privacy impact and accordingly changes should be made to the processes.
- This would require changes at every stage of the development lifecycle of business processes and new systems

Source: EUGDPR.org

Data Protection Officers (DPOs)

- DPOs must be appointed if an organization conducts large-scale systematic monitoring or processes large amounts of sensitive personal data.

Accountability

Organization must prove they are accountable by:

- Establishing a culture of monitoring, reviewing and assessing data processing procedures.
- Minimizing data processing and its retention
- Building in safeguarding to data processing activities.
- Documenting data processing policies, procedures and operations that must be made available to the data protection supervisory authority on request.

Mandatory breach notification

- Organizations must notify the supervisory authority of data breaches 'without undue delay' or within 72 hours, unless the breach is unlikely to be a risk to individuals.
- In case of high risk to individuals, they must be informed as well.

Source: EUGDPR.org


01-Sep-14
2000
1000

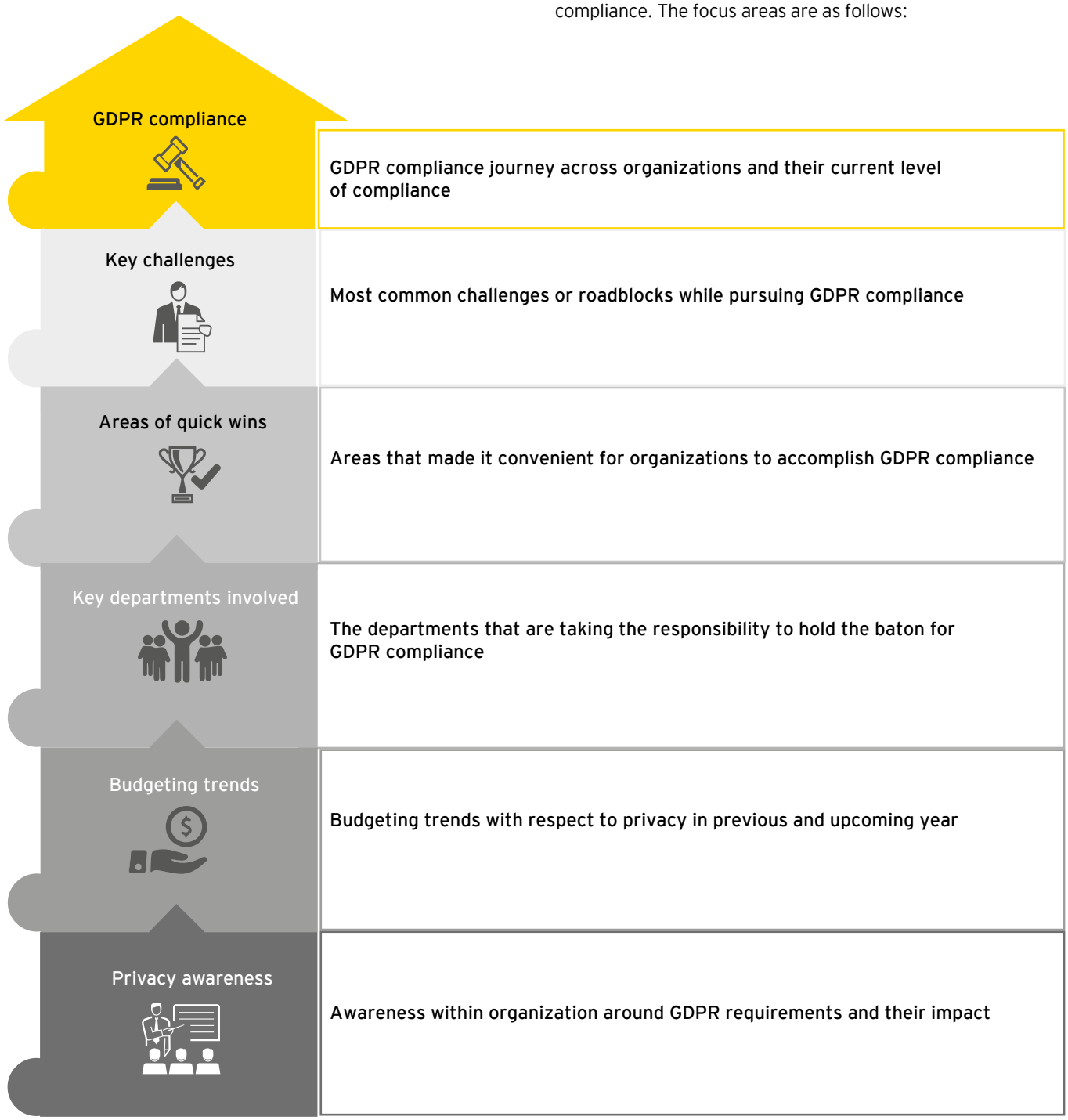
3 EY GDPR Readiness Survey

In a future where data is everywhere, who'll keep it out of the wrong hands?

EY commissioned a survey that captures the responses of 77 C-Suite leaders that include Privacy experts, legal heads and IT executives/managers, representing diverse industrial segments. These include many of the large globally recognized organizations as well as key government entities. The research was conducted between April – May 2018.

EU's General Data Protection Regulation (GDPR) aimed to usher in unprecedented levels of data protection for the EU residents and businesses across the globe. In order to get better insights towards the GDPR compliance journey of organizations across different sectors in India, EY conducted a survey.

The survey included a multitude of questions ranging from the organizations particulars to details about the privacy framework adopted by them and the initiatives taken towards GDPR compliance. The focus areas are as follows:

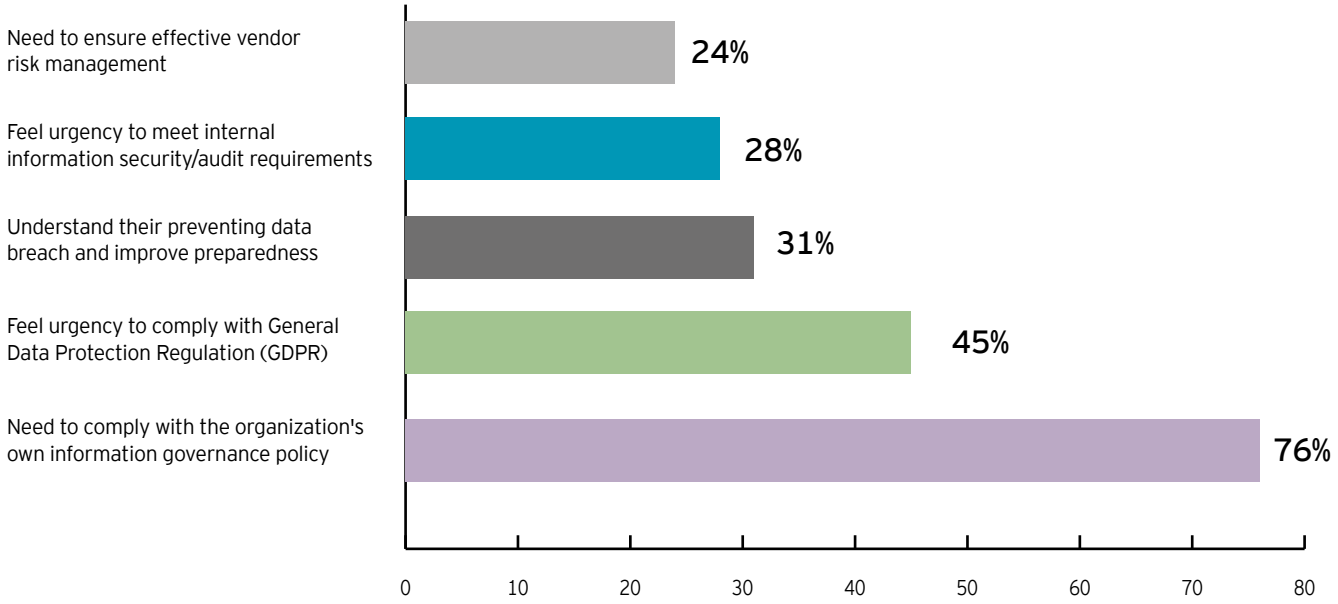


[11]http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Key Highlights of the EY GDPR Readiness Survey:

76% of the organizations identified the need to comply with their own information governance policies as the leading factor in their GDPR compliance journey

What are the main challenges faced by organizations in their GDPR compliance journey?



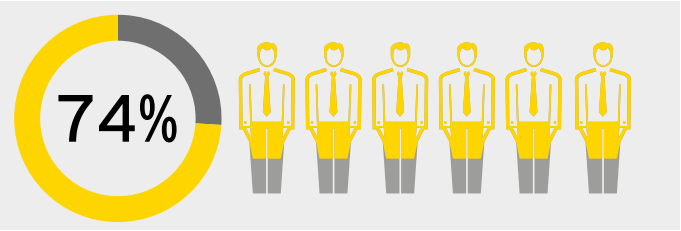
4 Key Survey Findings

Where does India Inc. stand in its GDPR compliance journey?

With GDPR coming into effect, the privacy landscape has changed dramatically. GDPR requirements and its stringent penalties have compelled all organizations to take privacy seriously.

GDPR compliance starts with GDPR awareness. Inadequate awareness continues to be a concerning factor. It already starts with GDPR awareness in scope of the legal aspects, the exact understanding of what GDPR encompasses and how to start prioritizing and planning to be as close to compliance as possible. There are still myriads of companies that struggle to understand the full impact and even its meaning.

In the Indian scenario, we observed an increased awareness wherein majority of the organizations as close to **74%** of them were aware of GDPR and its impact on them



This can be attributed to an increased effort by industry bodies and media which played a crucial role in GDPR awareness enhancement and can also be attributed to a push from their EU counter parts.

IT/ITeS sector has taken a lead in terms of its GDPR compliance and more than **50%** of the organizations to whom it is applicable are aware about GDPR and its impact on their organization. This can be attributed to an increased push from their customers.

The awareness needs to be further enhanced as approx. **26%** respondents from organizations for which GDPR is applicable (as they have customers/suppliers in the EU) are not aware of its requirements and impact.

1/4th of survey respondents belonging to organizations that are offering goods and services in the EU but still are being unaware of GDPR requirements and its impact, it not only poses a huge risk to protection of customer personal information, but also portrays the inability to demonstrate compliance to the applicable GDPR regulation.

The real question is not just about awareness but also about working in the right direction to achieve GDPR compliance

It is vital for all org/anizations that have applicability of GDPR as per their roles, of processors and/or controllers, to fulfil the mandatory requirements. Heeding to this call of trans-border privacy regulation, approx. **80%** organizations that are aware of GDPR have proactively initiated their compliance journey towards it.

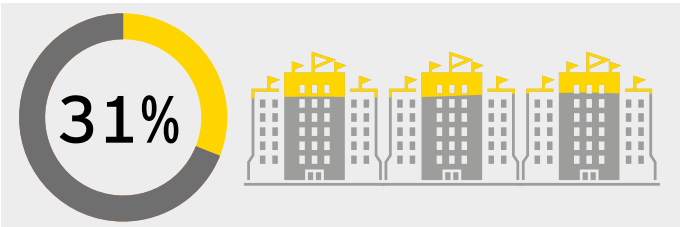
GDPR Compliance - Where does the responsibility lie?

According to the survey, over **63%** respondents who were aware of its requirements and impact said that they are non-compliant as on date.

While majority of them are aware of consequences of non-compliance to GDPR, they are yet to complete their compliance journey. There is a lot of ground that organizations must cover to ensure compliance to GDPR requirements.

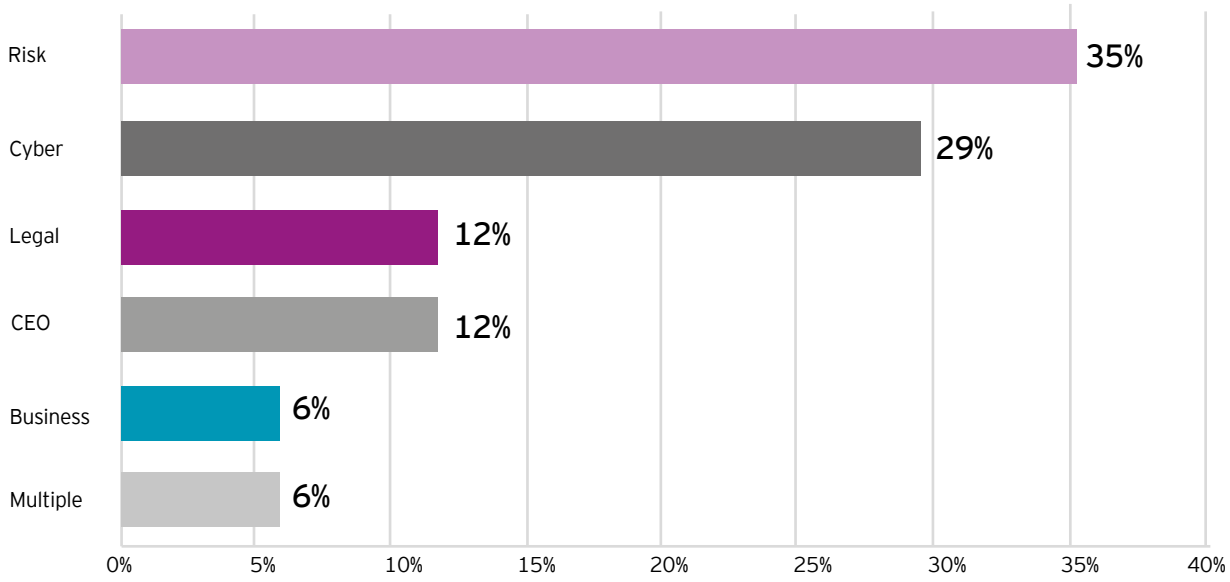
Of the **31%** organizations which believe that they are compliant, IT/ITeS organizations have taken a lead with **65%** belonging to this sector. This is followed by manufacturing and automotive organizations out of which **23%** believe that they are compliant with GDPR.

With IT/ITeS organizations leading the space of GDPR compliance, other sectors need to catch up.



Meeting GDPR requirements requires an in-depth understanding. In approx. **31%** of organizations which were GDPR compliant, cyber Security/Privacy and the risk compliance team lead with **35%** followed by cyber security at **29%,** who are responsible for performing the desired activities whereas in less than **12%** GDPR compliant organizations, legal team had taken the responsibility for the same.

Who is responsible for GDPR compliance within your company?



This is different from the global reports wherein legal /general counsel have been leading the way.

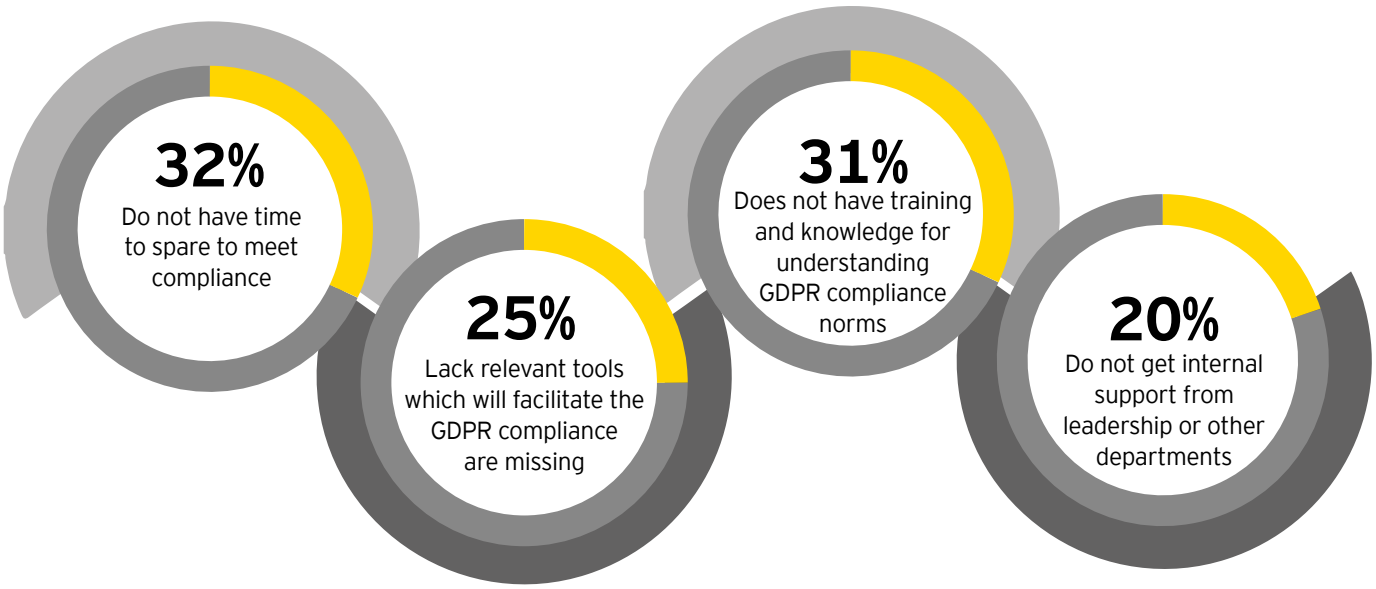
Key challenges encountered in GDPR compliance:

However, this journey is not a smooth sail for all organizations. Some organizations are facing a major challenge in getting adequate skilled resources and time from existing resources. More than **60%** of the organizations sighted these as the biggest challenge in performing GDPR compliance activities. Apart from finding individuals that have the right competencies, other challenges are also evident.

Skill and competencies should be gathered and appropriate stakeholders should be identified to successfully implement and carry forward any privacy program. In addition to having more skilled resources, organizations also acknowledged the need of having relevant tools which facilitate conduct of activities that help in ensuring the compliance. As the organizations conducting business in EU prepare themselves, GDPR also opens new avenues for product-based companies.

Approx. **50%** respondents stated that time/bandwidth was the most commonly stated reason for challenges faced by the organizations, followed by training and support from top leadership, whereas 25% of the organizations feel that the relevant ones that facilitate the GDPR compliance are missing.

What are the key obstacles that challenge an organization's GDPR compliance journey?



Key Strengths

In contrast to these issues , there are certain strengths that different organizations attribute to their privacy practices. The respondents believe that one of their major strengths that achieved their goal of addressing to the GDPR requirements include support from leadership, which was quoted as a primary reason, by approx. **54%**. This was followed by timely training and awareness as mentioned by **20%** of the respondents.

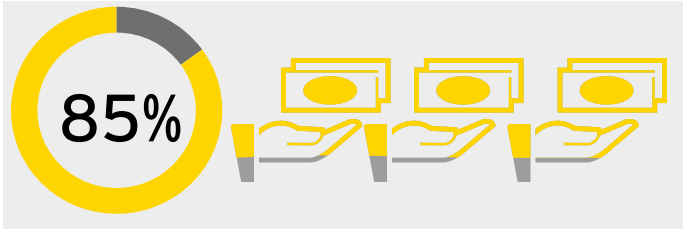
Organizations which successfully completed all the required activities for GDPR compliance gave the credit to leadership team for being supportive and the primary reason for being able to accomplish compliance to the regulation.

That's a very important message for the top management of the aspiring GDPR organizations. As the top management provides the support and strategic direction, there is also a dire need to train and enable the resources to enable them to perform the desired activities for the compliance.

Budget allocations

To meet new requirements improved privacy and information security budget allocations are also required.

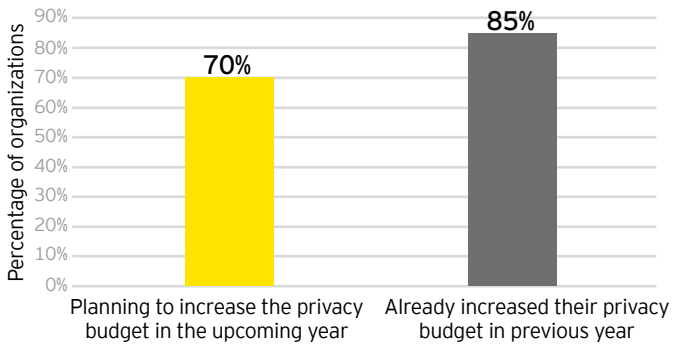
The industry is following this trend and an astonishing **70%** organizations, having more than 5000 employees, are planning to increase their privacy budget in the upcoming year.



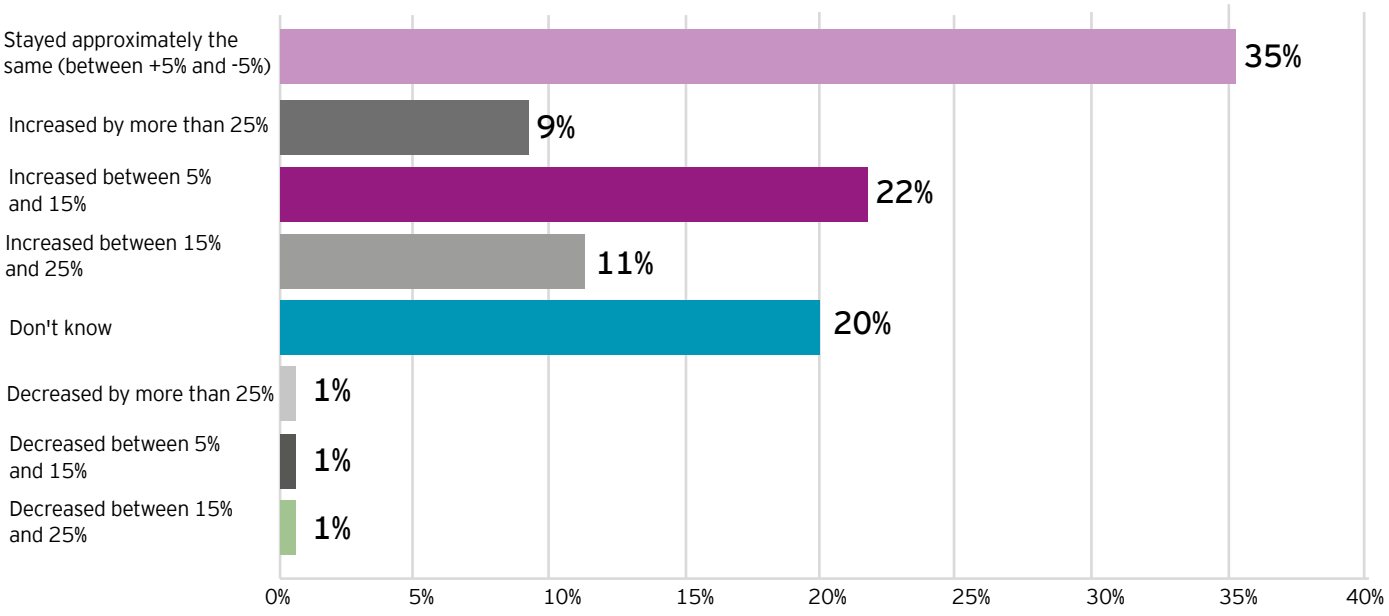
Over **85%** of organizations have increased their budget the in previous year and want to further enhance it in 2018.

As a matter of fact, every survey respondent belonging to a medium-sized organization (employee count between 1000-5000) confirmed that they are planning to increase their privacy budget by 5%-25%. The medium-sized organizations have also acknowledged the need to have controls to ensure privacy.

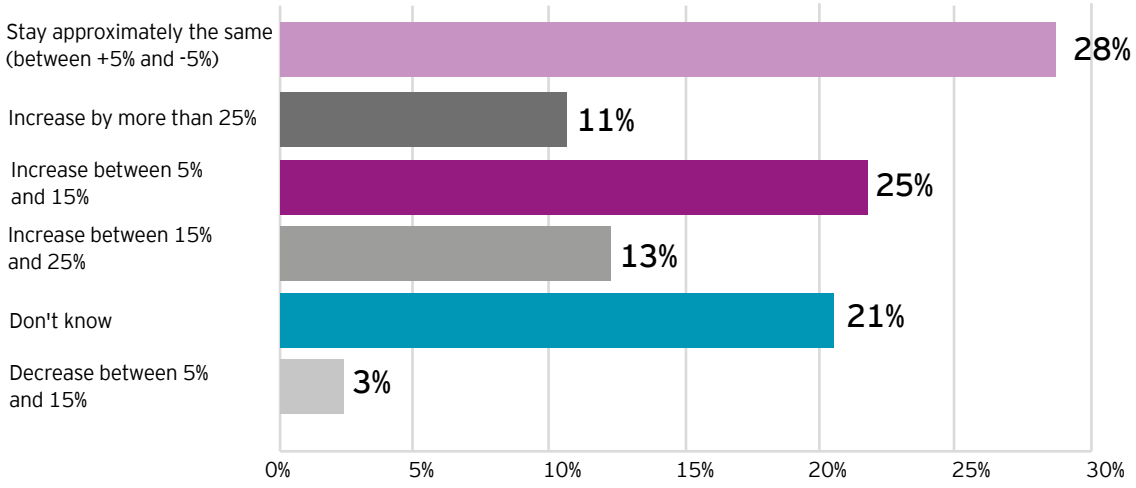
Predicted increase in privacy budgets every year, but is it enough?



How did the privacy budgets of organizations change in the past 12 months?



How are the privacy budgets of organizations expected to change in the next 12 months?



As, digitalization is on the boom, the need for new rules and regulations is dire to ensure safeguard of privacy of user/s. Approx. **50%** of respondents from organizations which neither have customers nor suppliers in the EU confirmed that their respective organization is planning to increase their privacy budget in the upcoming year.

This accounts for the acceptance of this dynamic environment of privacy and aligned regulations across the globe. Organizations are gearing up for any privacy law, new Data Protection law/ Amendment by Local Government including preparedness for any new rules and regulations that gives organization a hassle-free transition towards meeting compliance.

However, just increasing the privacy budget does not necessarily mean that the organization will meet the set requirements. Approx. **76%** organizations who had increased their privacy budget still are non-compliant.

The budget allocation should be well-managed and as per the privacy program implemented or to be implemented at any organization. More budget investment should be done towards creating awareness regarding privacy, general practices and employee obligations. This is vital in the sense that human resource is one of the most critical and crucial components of the privacy program that enables the practices to be followed by the organizations.

5 Data privacy and GDPR: a forensic perspective

We live in a world of wide-ranging surveillance. Historically, this has been expensive and difficult to comprehend. However today with technology, surveillance has advanced in leaps and bounds with its tentacles surrounding every aspect of the current virtual world, wherein everything is either collected, saved, analysed or searched over the internet. While technology has streamlined processes, and given rise to new business models, it has also increased vulnerabilities around data theft, privacy and protection.

Mission information protection

A recently reported high-profile case in the media and the subsequent government and public scrutiny around it has once again brought the prominence of enacting and enforcing data protection and privacy laws into light. India also has been taking strides to protect data in this digital time and age. The Supreme Court of India declaring the "Right to Privacy" as a fundamental right, is being considered a landmark judgement to bring in substantial changes into how data is considered, used and deliberated. Additionally, the introduction of Data (Privacy and Protection) Bill, 2017 proposes to streamline user data protection by setting up a data privacy and protection agency. EU's GDPR will make businesses in India accountable and responsible for EU citizens' Personally Identifiable Information (PII) as non-compliance or data breach can lead to severe warnings and penalties.

Ambiguity around data privacy laws prevail

The Government has been introducing new laws and amending the existing ones. Sectoral regulators such as IRDAI, SEBI, TRAI, CCI etc. are also understanding the importance of data protection and have been talking about maintaining privacy. However, awareness around cyber laws is still lacking. Most organizations and individuals are still struggling to understand even the basic provisions of laws around data privacy.

Today, there is a dire need for organizations in India to find methods on how best to achieve 'informed consent' from the masses and at the same time ensure greater awareness around reforms and legislations. Globally, this is taking place at a rapid pace and Indian companies and businesses will need to match up to global standards to mitigate potential data breaches, boost awareness and reduce legal ease.

GDPR – a strategic business opportunity

Organizations can either look at GDPR as a burden or an opportunity to build stronger compliance mechanisms for better data governance. While many EU corporations are grappling with the changes; organizations in other regions such as Asia, Africa and US holding EU data also need to be compliant. Implementation will offer many strategic opportunities that may align with other existing business initiatives. Revamping and reorganizing data can be done through an Information Governance Program which will bring in a structure, offer accountability of ownership and enhance understanding of data existence, location and server management. Benefits include –

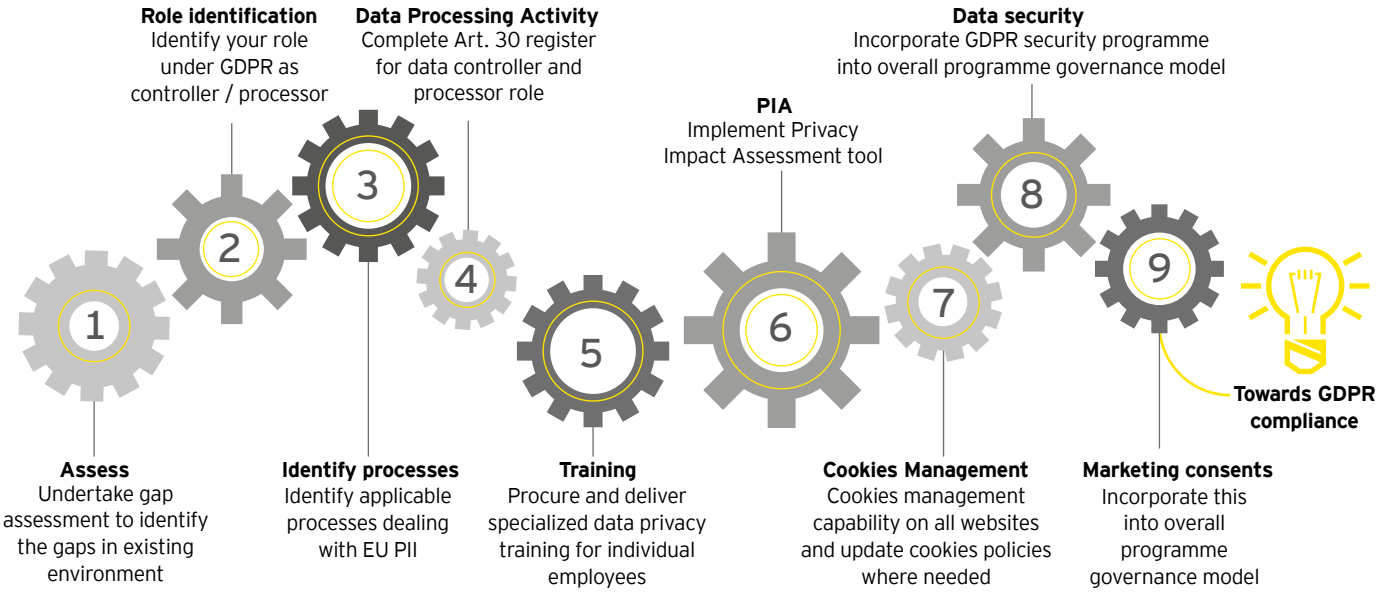
Organizations can either look at GDPR as a burden or an opportunity to build stronger compliance mechanisms for better data governance. While many EU corporations are grappling with the changes; organizations in other regions such as Asia, Africa and US holding EU data also need to be compliant. Implementation will offer many strategic opportunities that may align with other existing business initiatives. Revamping and reorganizing data can be done through an Information Governance Program which will bring in a structure, offer accountability of ownership and enhance understanding of data existence, location and server management. Benefits include –

- Improving visibility of customer privacy data:
  - Increases cyber protection effectiveness
  - Reduces risk and compliance concerns
- Adopting a global approach beyond EU:
  - Could simplify compliance efforts
  - Lowers risk of potential lawsuits
  - Strengthens privacy brand
- Improving cross-functional information flows and cross-system reporting could deliver new insights in:
  - Post-marketing surveillance
  - Supply chain efficiencies
  - Return on sales and marketing spend
- Disposing of junk data:
  - Reduces compliance data volume scope
  - Improves operational efficiencies
  - Realize an aggressive return on investment
- New data maps could streamline:
  - Insider threat focus and detection
  - Breach response
  - e-discovery and legal hold
  - Knowledge management
- Creating PII inventories across the enterprise allows for other critical information assets to be tracked to assist with broader risk and compliance concerns

In spirit, GDPR will impact nearly every facet of an organization and presents an opportunity for most businesses to fundamentally transform and improve their internal processes and drive more effective utilization of data – all while enabling compliance.

6 Way forward

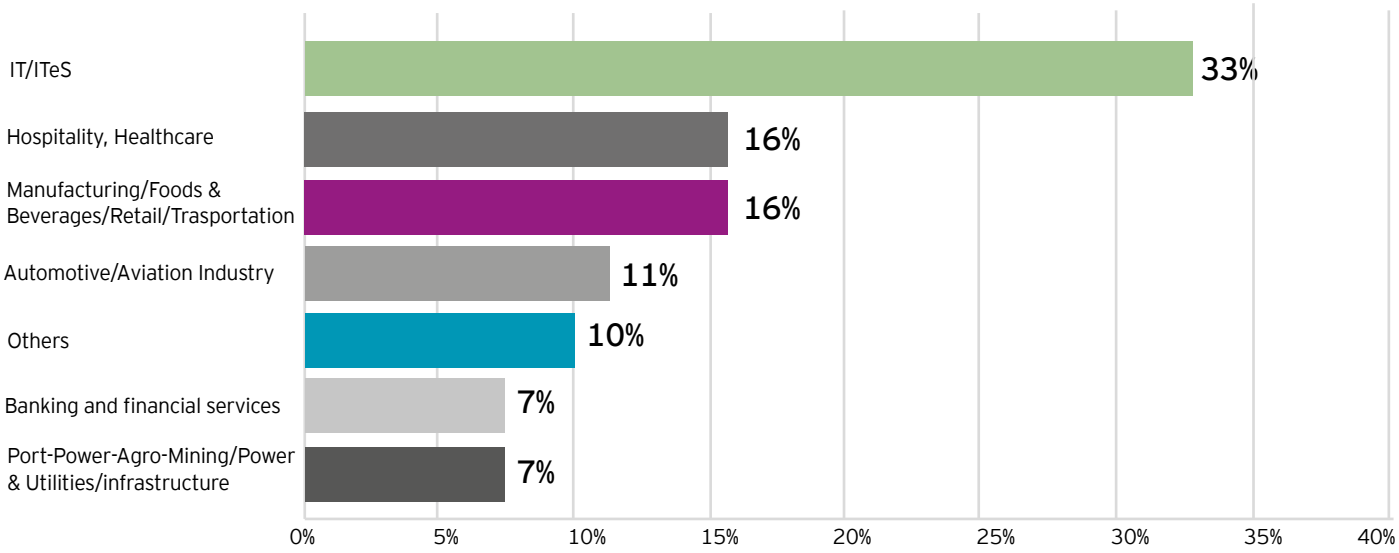
The organizations that have started their journey should continue to meet the needs of the regulation and shall also work towards identifying other privacy regulations which are applicable to them and ensure that the privacy framework is agile and can be customized to the needs of the changing environment. For the organizations which are yet to start their journey, it is recommended that they should do so at the earliest and work towards complying with the regulation. At a minimum both set of organizations may follow the above steps.



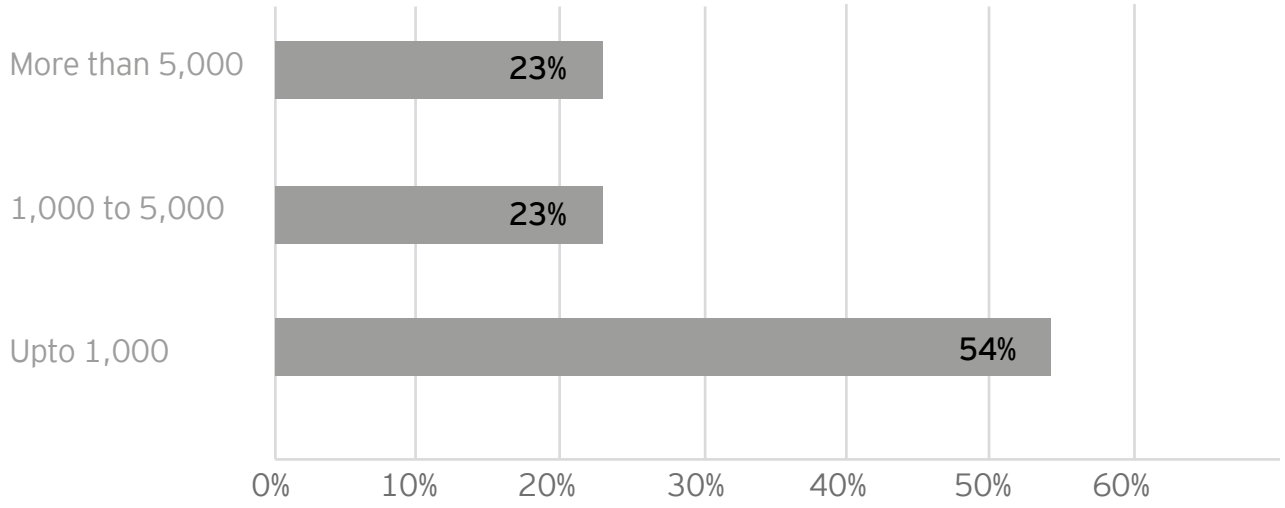
Survey methodology

EY commissioned a survey that captures the responses of 77 C-Suite leaders that include Privacy experts, legal heads and IT executives/managers, representing diverse industrial segments. These include many of the large globally recognized organizations across IT and ITes, Healthcare, Pharmaceuticals, Automotive, Media and Entertainment, Banking and Financial services. The research was conducted between April – May 2018.

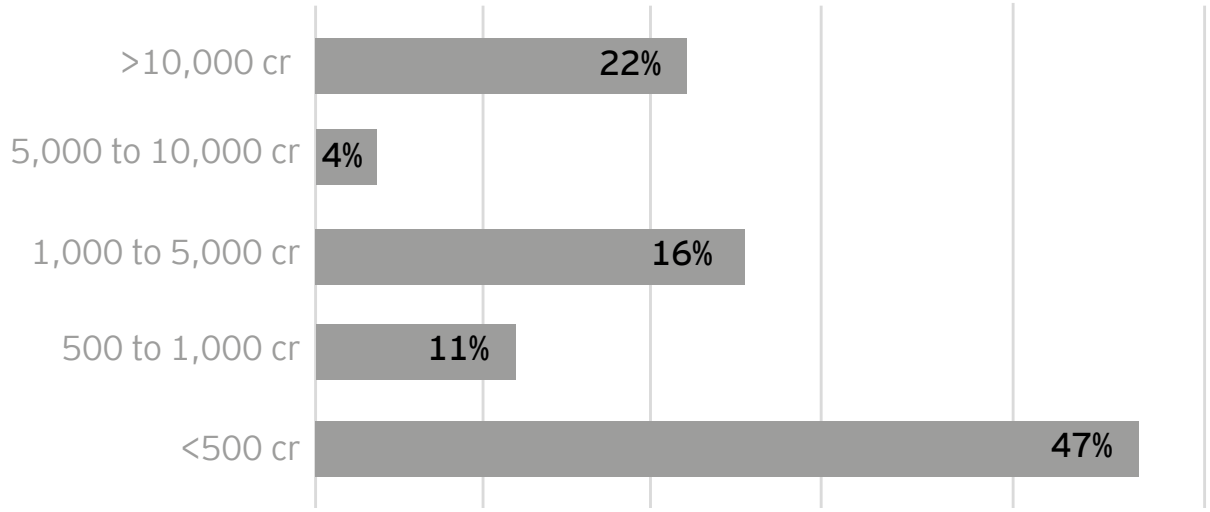
Respondents by sectors



Respondents by number of employees



Respondents by aggregate annual revenue



For any queries related to privacy or GDPR compliance, please contact:

EY Cyber Security and Data Privacy Services:

Burgess Cooper
Partner - Cyber Security, EY
Email: Burgess.cooper@in.ey.com
Contact: +91 22 6192000

Jaspreet Singh
Partner - Cyber Security, EY
Email: Jaspreet.singh@in.ey.com
Contact: +91 124 6714310

Vidur Gupta
Partner - Cyber Security, EY
Email: Vidur.Gupta@in.ey.com
Contact: +91 124 6711380

Tiffy Isaac
Partner - Risk Advisory, EY
Email: Tiffy.Isaac@in.ey.com
Contact: +91 80 67275016

Thomas Mathew
Associate Partner - Risk Advisory, EY
Email: Thomas.Mathew@in.ey.com
Contact: +91 80 67275054

Lalit Kalra
Senior Manager - Risk Advisory, EY
Email: Lalit.kalra@in.ey.com
Contact: +91 124 4434000

Sujay Maskara
Senior Manager - Risk Advisory, EY
Email: Sujay.Maskara@in.ey.com
Contact: +91 80 6727 5912

EY Forensic & Integrity Services:

Arpinder Singh
Partner and Head - India and Emerging Markets Forensic & Integrity Services EY
Email: arpinder.singh@in.ey.com
Contact: +91 12 4443 0330

EY offices

Ahmedabad
2nd floor, Shivalik Ishaan
Near C.N. Vidhyalaya
Ambawadi
Ahmedabad - 380 015
Tel: + 91 79 6608 3800
Fax: + 91 79 6608 3900

Bengaluru
6th, 12th & 13th floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 4027 5000
+ 91 80 6727 5000
+ 91 80 2224 0696
Fax: + 91 80 2210 6000

Ground Floor, 'A' wing
Divyasree Chambers
11, O'Shaughnessy Road
Langford Gardens
Bengaluru - 560 025
Tel: +91 80 6727 5000
Fax: +91 80 2222 9914

Chandigarh
1st Floor, SCO: 166-167
Sector 9-C, Madhya Marg
Chandigarh - 160 009
Tel: +91 172 331 7800
Fax: +91 172 331 7888

Chennai
Tidel Park, 6th & 7th Floor
A Block (Module 601,701-702)
No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100
Fax: + 91 44 2254 0120

Delhi NCR
Golf View Corporate Tower B
Sector 42, Sector Road
Gurugram - 122 002
Tel: + 91 124 464 4000
Fax: + 91 124 464 4050

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 6671 8000
Fax + 91 11 6671 9999

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Noida - 201 304
Gautam Budh Nagar, U.P.
Tel: + 91 120 671 7000
Fax: + 91 120 671 7171

Hyderabad
Oval Office, 18, iLabs Centre
Hitech City, Madhapur
Hyderabad - 500 081
Tel: + 91 40 6736 2000
Fax: + 91 40 6736 2200

Jamshedpur
1st Floor, Shantiniketan Building
Holding No. 1, SB Shop Area
Bistupur, Jamshedpur - 831 001
Tel: +91 657 663 1000
BSNL: +91 657 223 0441

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 304 4000
Fax: + 91 484 270 5393

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400
Fax: + 91 33 2281 7750

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 1000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E),
Mumbai - 400 063
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 3000

Pune
C-401, 4th floor
Panchshil Tech Park
Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 6603 6000
Fax: + 91 20 6601 5900

Notes

Notes

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

EYIN1808-001
ED None

RB

About EY's Advisory Services

About EY's Advisory Services In a world of unprecedented change, EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses. From C-suite and functional leaders of Fortune 100 multinationals to disruptive innovators and emerging market small- and medium-sized enterprises, EY Advisory works with clients – from strategy through execution – to help them design better outcomes and realize longlasting results. A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions. They work with their clients, as well as an ecosystem of internal and external experts, to create innovative answers. Together, EY helps clients' businesses work better

About EY's Forensic & Integrity Services:

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

ey.com/in

@EY_India EY|LinkedIn EY India EY India careers ey_indiacareers