



GDPR Preparedness Survey Report

For private circulation only

June 2018

Contents

Foreword	05
Executive Summary	06
1: Introduction	08
2: Applicability of GDPR to Indian organisations	10
3: Early starters	14
4: Drivers to be GDPR ready	18
5: Strategy and Governance	22
6: GDPR Implementation	26
7: Maintaining concurrence with GDPR	36
8: Data transfer between India and EU	42
9: State-of-the-art measures	46
About Deloitte	49
About DSCI	50





Foreword

India has emerged as a global service hub and has been a partner of choice in the digital transformation journey of global enterprises across 100+ countries. European Union (EU) has been a key geography for the Indian industries such as IT, manufacturing, healthcare, retail etc. which have been serving customers across several verticals and business functions.

Innovations in global service delivery models, best in class processes and standardization has kept India's service industry growth story flying high. Maintaining its much-coveted position as world's leading global delivery hub, India continues to scale its global delivery with innovation in business models, hyper specialised services and process maturity. Conformance to data protection regulations in various geographies has been enabled by advancements in Data Protection and harnessing technology solutions for rigorous implementation globally.

Given the recently enforced EU GDPR, stepping-up focus on data protection practices is a key requirement to satisfy expectations of global customers and consumers.

Over the last two years, Deloitte and DSCI have engaged with their clients and members respectively in their GDPR readiness journey. With the main objective of generating awareness, assessing GDPR readiness, understanding the evolving best practices and learnings, and to take stock of gaps (if any) and identify improvement areas, DSCI and Deloitte worked hand-in-hand to roll out the GDPR readiness survey to members of Indian industry servicing/operating in the EU geography. The result is a report encapsulating the survey findings that will enable adoption and sharing of best practices and delineation of the next steps for scaling up GDPR readiness.

Executive Summary

Data Security Council of India (DSCI) and Deloitte Touché Tohmatsu India LLP (DTTILLP, or Deloitte) jointly conducted a survey to study the preparedness of organisations based in India with the requirements mandated by the European Union's (EU) General Data Protection Regulation (GDPR)¹. The objective of this survey was to measure the GDPR readiness process and the overall alignment towards privacy of Indian organisations. The report details many aspects such as the awareness of the Indian organisations, how GDPR would be applicable to them, how they are preparing for it, what are few of the most prevalent leading practices used by Indian organisations to adhere with the requirements laid down by the regulation.

Almost one third of organisations who responded to the survey offer services and have presence in the EU. As compared to large Indian organisations (with employee count of more than 10,000), majority of Indian Small & Medium Enterprises started their GDPR readiness journey towards late 2017. From sector perspective, IT/BPM, Health and E-commerce were identified as the frontrunners of the GDPR readiness journey. Based on the survey results it was identified that the primary driving factor for GDPR readiness was to avoid legal & contractual liabilities, fines & penalties followed by gaining a competitive advantage through GDPR compliance. Another related aspect that was identified was for organisations to have a dedicated privacy team with increase in privacy laws and regulations around the world. As an initial step towards adopting a privacy culture, organisations are looking to prioritize training and hiring the right privacy workforce to manage

¹ The GDPR is a sector-neutral and border-less regulation. Along with organisations in the EU, it is also applicable to organisations based outside the EU that are handling personal data of the EU data subjects under given conditions of application.

and implement the requirements of GDPR and defining data classification policies and procedures.

Further the survey results indicate that Indian organisations prefer to establish a clear and legitimate purpose for processing personal data in a transparent, fair and lawful manner. It was noted that personal data was being collected mostly in the forms of online identifiers, location data and directly identifying data, whereas sensitive data was being collected in the form of biometrics or health data. The leading grounds of processing such personal and sensitive data were performance of contract' and consent, with electronic and written forms being the most used mediums for explicit consent.

Majority of the Indian organisations consider "Principles relating to processing of personal data (Ref: Article 5, GDPR)" as an enabler of a privacy oriented ecosystem in an organisation and not a hindrance. However, a few requirements such as a data subject's right to data portability, erasure and other restrictions on processing pose a challenge to the current setup of Indian organisations.

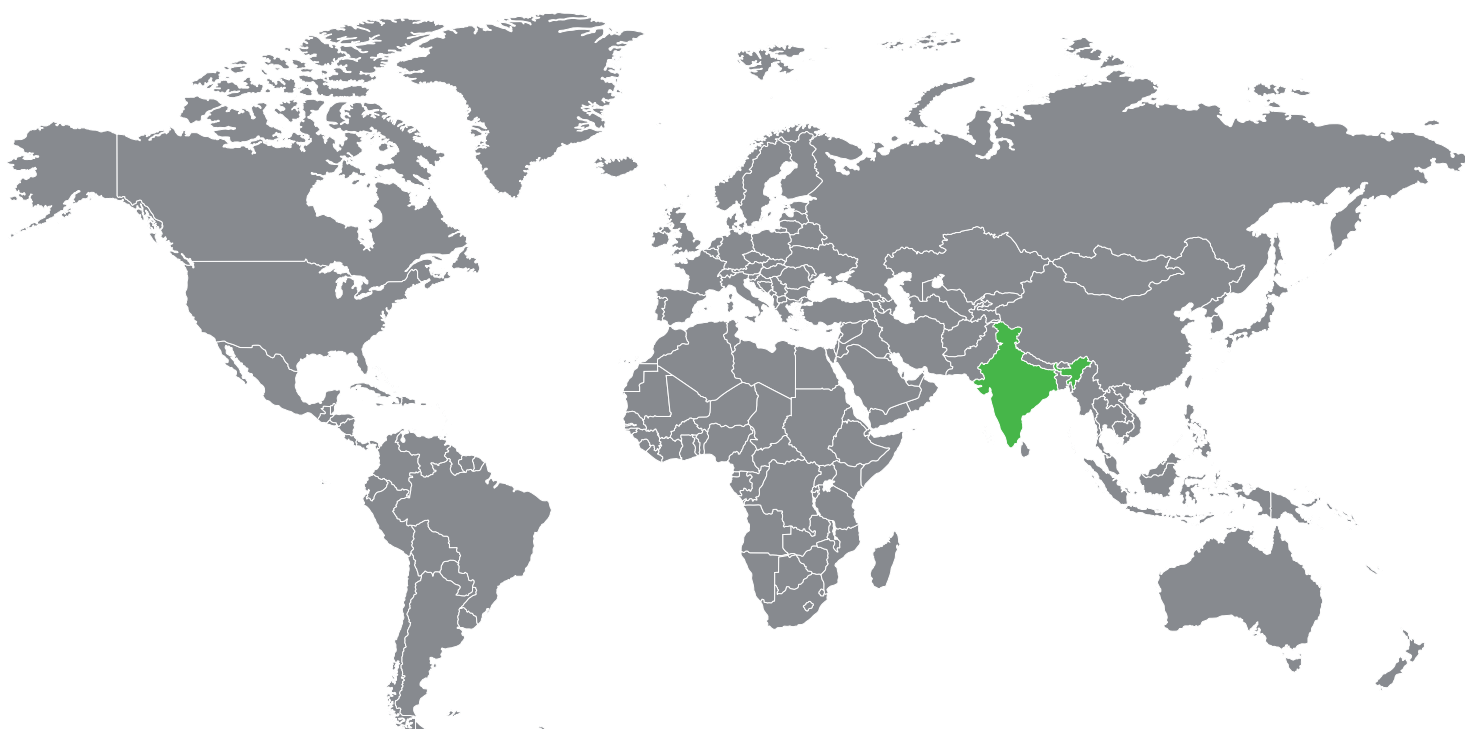
Few more challenges for maintaining concurrence with GDPR such as record keeping, Data Protection Impact Assessment (DPIA) etc. were also discussed. Since complying to GDPR is not a one-time activity, organisations will have to adhere to certain obligations on a regular basis. Amongst such obligations, maintaining records for processing activities proved to be more tedious for organisations having substantial number of employees or processing large amounts of data.

Another viewpoint that was noted was with respect to appointment of a Data Protection Officer (DPO) which was relative to size of an organisation. Large organisations were appointing / or keen to appoint a DPO preferably having a legal qualification whereas small organisations were appointing /or keen to appoint their business head or CIO as a DPO.

With respect to Data breach notification requirements, the survey indicates that the organisations functioning as controllers were more focussed on procedural arrangements for notifying a data breach at the earliest while processors were concerned about reporting a Data breach.

This survey also covered the aspect of cross border data transfer. India, at the moment is not an adequate nation for cross border transfers with the EU. Securing this status would open up a plethora of opportunities for Small & Medium Enterprises. In its absence, Indian organisations have widely been using Instruments such as Standard Contractual Clauses (SCC) and Binding Corporate Rules (BCR) to facilitate cross border data transfer.

The report concludes by highlighting the leading State-of-the-art security measures used across Indian industries, with data centric measures such as encryption, email security, data leak prevention being more prevalent at present whereas consumer centric measures slowly being adapted as the society becomes more aware and vigilant towards protection of their personal data.





01

Introduction

Background

The world is an ever-shifting paradigm of resources and the latest resource proving pivotal for every organisation is 'Data'. Advancements and technological innovations such as Internet of Things (IoT), Artificial Intelligence (AI), etc. are triggering a digital revolution all over the world but consequently raising a need to manage the associated digital risks. One of such risks pertain to the use of personal data that could potentially harm the data subjects. To control the increasing risk related to personal data, governments and regulators around the world are working towards strengthening privacy legislations. One of the most significant and recent developments in this era was adoption of General Data Protection Regulation (GDPR) (EU) 2016/679 by the European Union (EU) in April 2016 and its enforcement from May 25, 2018. GDPR focuses on safeguarding the personal data of data subjects within the EU and discourages use of their personal data beyond agreed purpose. This regulation has replaced the Data Protection Directive 95/46/EC and harmonizes data privacy laws across Europe, to protect personal data of EU data subjects and empowers them with rights associated with the use of their personal data. Its extra territorial

coverage expects personal data of EU data subjects to be safeguarded within and outside the EU, and thus this survey was conducted to study the GDPR readiness of Indian organisations processing the personal data of EU data subjects.

Many Indian Multi- National Organisations (MNCs) that have operations in the European Economic Area (EEA) or have business interests in that region have been approached by their vendors, employees, clients to respond on queries related to GDPR readiness. The survey revealed that Indian organisations are gearing up for GDPR by adopting leading practices to monitor, assess and manage privacy related risks.

Subsequent sections provide insights based on the response provided by the participants to the survey questionnaire. The results of this survey indicated that organisations pursue a wide range of readiness approaches towards GDPR.

Methodology

The DSCI – Deloitte GDPR readiness survey report was made with a comprehensive methodology to obtain deeper insights of the industries

with respect to GDPR. The initial step constituted a thorough situational analysis for model development. This was supported by identifying information needs for this particular research objective. Qualitative research was supported with secondary research on the nuances of GDPR to ascertain the various Variables of Interest (VOI) from an organisation's point of view. The questionnaire was designed to entail the aforementioned set of VOIs found. The survey was rolled out for two months from 12 March 2018 till 9 May 2018. The quantitative research comprised of a detailed analysis of the survey responses to secure correlations of the VOIs. These findings were then combined with secondary research to derive inferences with respect to GDPR and the organisations under its applicability.

Survey participants

The survey results are based on responses from 58 participants. The participants represented small to large sized organisations and diverse sectors such as Information Technology (IT)/Business Process Management (BPM), Banking Financial Services and Insurance (BFSI), Telecommunications, Manufacturing, Pharmaceuticals, Healthcare, and Oil & Energy.

Objectives

The survey was designed to address the following objectives: -



To study the readiness of Indian organisations against the EU GDPR



To check awareness amongst Indian organisations about GDPR



To provide key insights on various trends and correlations between GDPR requirements and overall privacy postures of Indian organisations



To provide an overview of leading practices followed by organisations



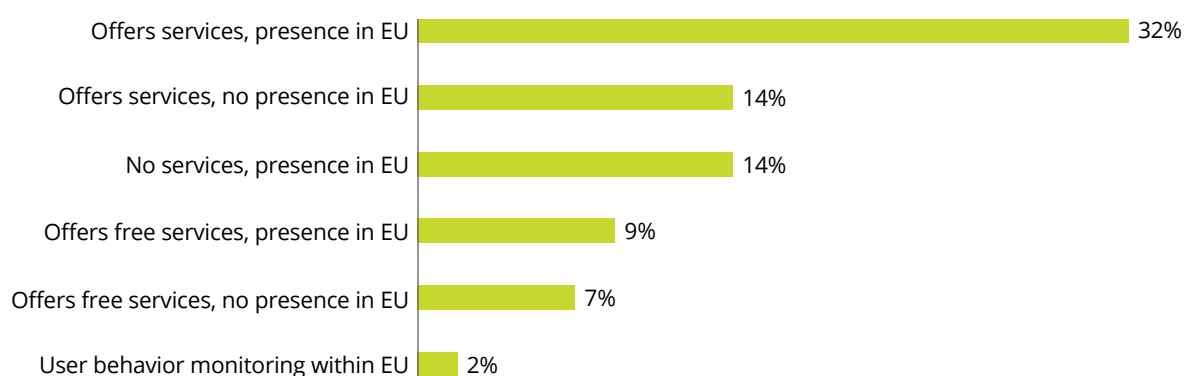
02

Applicability of GDPR to Indian organisations

As mentioned in Chapter 1, GDPR's extra territorial coverage impacts organisations beyond the EU, including the organisations in India process personal data of EU data subjects². During the survey, it was observed that some Indian organisations were not sure whether GDPR applies to them or not. In such cases, the first step would be to understand GDPR's applicability criteria and to simplify its applicable to organisations process personal data irrespective of physical presence (within or outside the EU). Based on the survey results, it was noted that for ~55% of Indian organisations, GDPR applies to them because of local presence in the EU (including organisations offering free services or no services in the EU).

1. Applicability as per activities of an organisation

Most prevalent activities in organisations



Almost one third of the organisations offer services and have presence in the EU.



Survey result

The above chart indicates that 32% of the respondents offer services and have presence in the EU as compared to 14% of the respondents who do not have presence in the EU but offer services.

Extra-territorial scope of GDPR applies to 23% of organisations by providing goods & services to individuals or monitoring behaviour of EU remotely from India.



² 'data subject': an identifiable natural person is one who can be identified, directly or indirectly;

Insight

GDPR is a borderless law and is expected to be enforced by a network of supervisory authorities/ regulators in the EEA. Therefore even if an Indian organisation does not have local operations in a particular EEA country, GDPR may still be applicable. Below are sample scenarios:

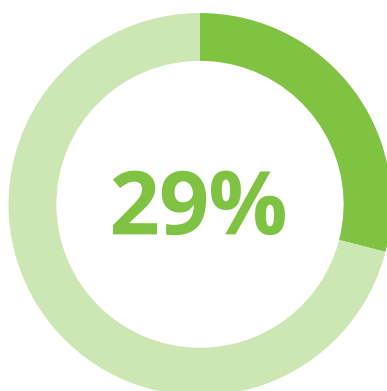
1. Indian organisations having a physical presence in EEA, and registered with the local supervisory authority / regulator, can be made to comply with notices, site inspection by the authority, etc.
2. Indian organisations with no physical presence in EEA, directly providing customer services to data subjects in EEA, may require an EU representative. An EU representative would represent its Indian organisation in front of the local regulator and may establish a channel for enforcement and compliance requirements.
3. Indian organisations with no physical presence in EEA, indirectly providing customer services to data subjects in EEA. For an Indian organisation operating as a sub processor or as a data processor to a data controller within the EU, GDPR will be enforced via the binding clauses in service contracts.

Once applicability is established, it is important to assess the organisation's role i.e. a Data Controller³, or Joint Controller⁴ or Data Processor⁵ or Sub Processor⁶. Survey results indicate that ~51% of Indian organisations are operating as Data Processor.

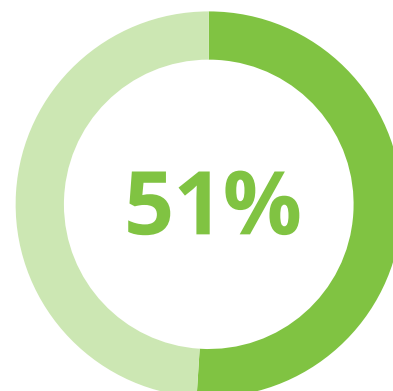
2. Roles of organisations W.R.T. GDPR



Direct legal liability
(Controllers)



Contractual liability
(Sub-processors)



Mostly contractual, legal in certain
circumstances (Processors)

Majority of the Indian Organisations are Data Processors.



Survey result

The survey highlighted that 20% of the respondents operate as a controller since they have a direct legal liability for all activities involving its collected personal data. A processor has mostly contractual liability and a legal liability in some circumstances, whereas a sub processor has solely a contractual liability.

³ 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

⁴ Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

⁵ 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

⁶ Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act

Detailing this result further, the table below represents sectoral coverage of organisations operating as Controller, Sub-processor, and Processor.

Direct Legal liability (Controller)	Contractual liability (Sub-processor)	Mostly contractual, sometimes legal (Processor)
Indian MNC (operating in the EU) (60%) BPM (67%) Call Centre (60%)	Engineering Services (43%) Internet Platforms (67%) Consulting (39%)	IT Services (42%) MNC IT Services (50%) Global In-house Centre (67%) KPO (50%) Technology Product (41%)

Myths around applicability

It was noted that the Business Process Management (BPM) organisations, call centres, and Business Process Outsourcing (BPO) organisations perceived themselves to be data controllers. However, it's a myth as such organisations are actually data processors as they do not determine the purpose and means of processing personal data of EU data subjects. They are bound by a service contract with their respective client (likely to be a data controller) to process the data in a specified sequence/steps and share the results of processing. It is important for Indian organisations to assess their role under GDPR, i.e., a Data Controller (DC), Data Processor (DP) or both, since regulatory requirements from a DC may vary from those for a DP.

To conclude, the results in this chapter clearly indicate that GDPR, although a European regulation, significantly impacts Indian organisations. The next chapter analyses when such Indian organisations started their GDPR readiness journey and what factors influenced it.



03

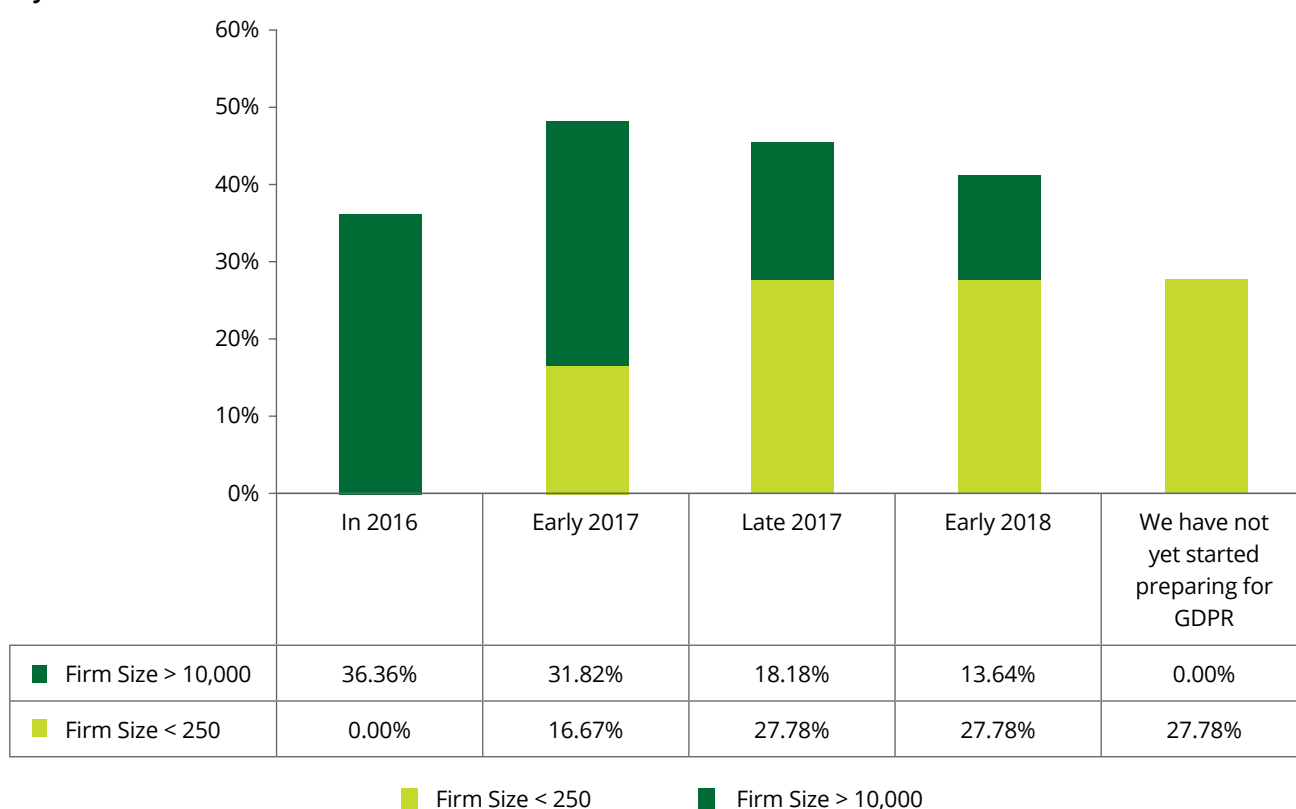
Early starters

In 2016, the EU Regulation on Data Protection (GDPR) was published in the Official Journal of the EU. The GDPR was adopted on 24 May 2016 and replaced the former 1995 EU Data Protection Directive to create a harmonised data protection law across Europe. Organisations around the world were given a two year period to get themselves ready before GDPR was enforced from 25 May 2018.

The survey revealed that in India, organisations reacted to GDPR in different ways. Almost 21% started GDPR readiness journey in 2016 while 17% were yet to embark their GDPR journey. It was also noted that only large organisations (with over 10,000 employee count) were early starters and embarked their GDPR readiness journey in the year 2016 itself as compared to small organisations (with less than 250 employee count), which started in 2017-18.

3. Size of the organisation vs the GDPR journey

Journey towards GDPR



Majority of Indian Small & Medium Enterprises started their journey late as compared to Big Indian organisations.



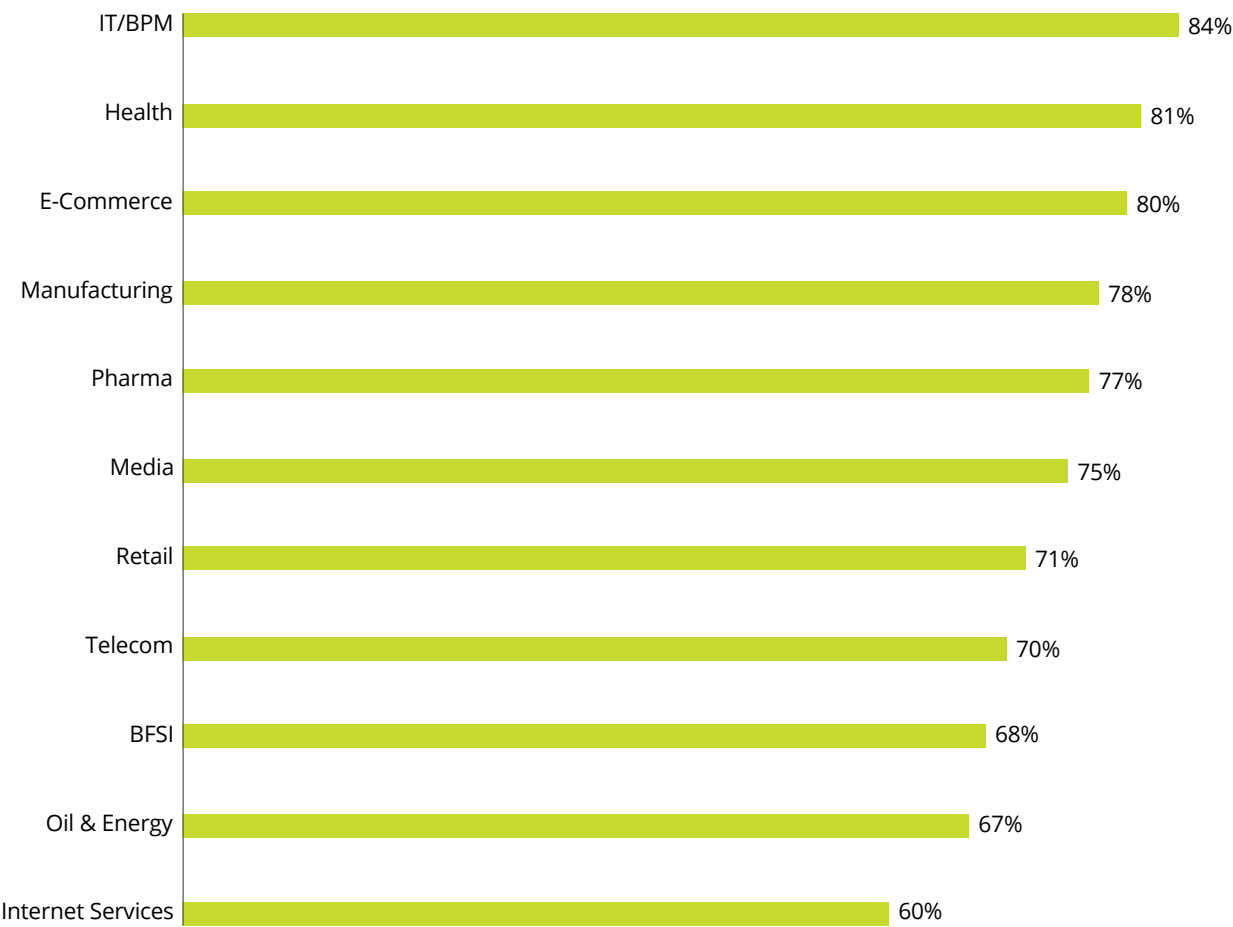
**Survey
result**

By early 2018, all large organisations (size > 10,000) had started their GDPR readiness journey, with majority (36%) of large organisations initiating it in the year of GDPR declaration itself (2016). On the other hand, around 28% of the small organisations were yet to initiate their journey towards GDPR as they face issues due to many reasons such as lack of dedicated privacy team or insufficient/no budget allocation for the readiness program, etc.


It was also noted that apart from organisational size, the sector in which organisation operate also determined the time when they started their readiness journey. The sectors that led GDPR readiness efforts were IT/BPM, Health, Ecommerce, Manufacturing and Pharma. It was inferred that sectors which handled lesser amounts of personal data weren't very prompt and comparatively had a slow start towards GDPR readiness.

4. Initiation of GDPR readiness – sector wise

Sectoral depiction of organisations that have started their GDPR journey



IT/BPM, Health and E-commerce were the frontrunners of the GDPR readiness journey.



Survey result

The Sectoral depiction clearly indicates that IT/BPM sector was the most responsive sector in terms of taking any steps towards GDPR readiness with 84% of IT organisations having started their readiness journey. This is followed by health and E-commerce sectors with 81% and 80% organisations respectively initiating their process.



To conclude, the **size** and the **sector** were two key factors that determined prompt or slow response of Indian organisations towards GDPR readiness. The subsequent chapter, highlights the impetus for Indian organisations to be GDPR ready.



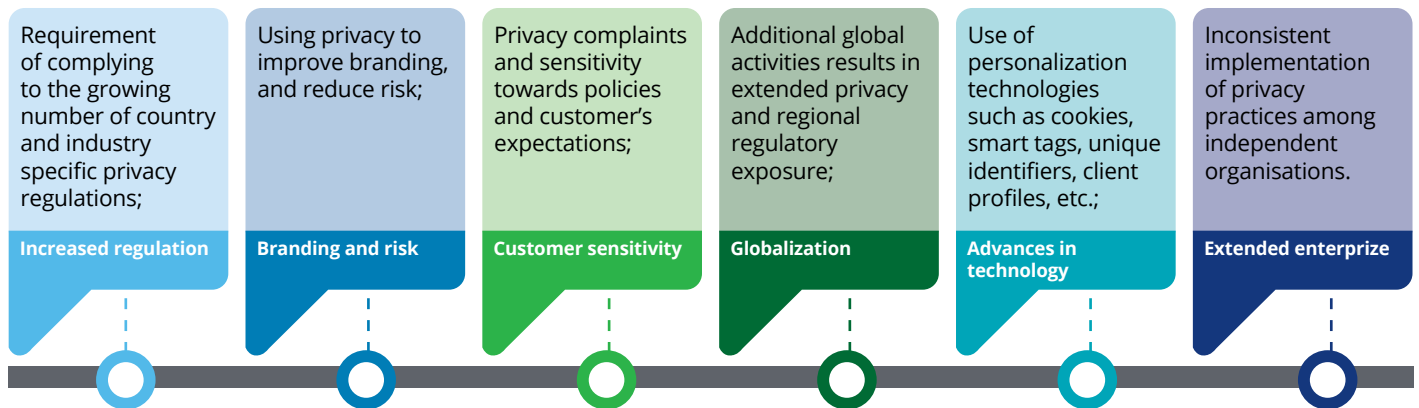


04

Drivers to be GDPR ready

Subsequent to the GDPR enforcement date which is 25 May 2018, more and more organisations from every sector are looking to be GDPR ready; however, across organisations, the motives vary.

Investing in GDPR readiness and, further, in privacy, is motivated by some of the following factors:



The survey provided participants with multiple objectives and reasons to be GDPR ready. With the option to select all applicable reasons, the top three reasons for Indian organisations to be GDPR ready are:

62%

Avoiding legal & contractual liabilities, fines and penalties is the key focus

60%

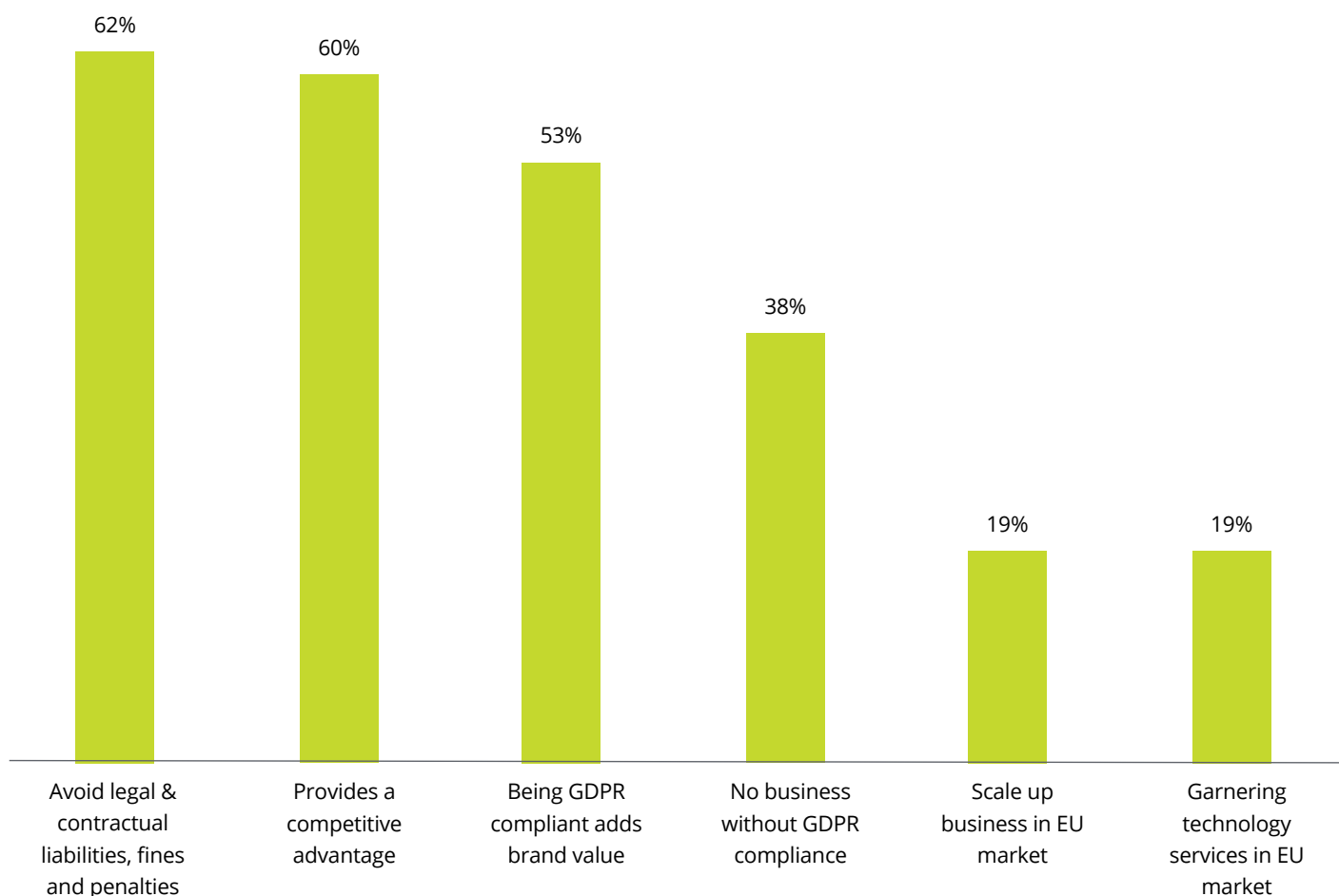
GDPR compliance provides us a competitive advantage in the market

53%

Being GDPR compliant adds to our brand value



5. Motivation factors for GDPR readiness



Leading factors towards GDPR readiness were to 'avoid legal & contractual liabilities, fines and penalties' and to have a 'competitive advantage'



Survey result

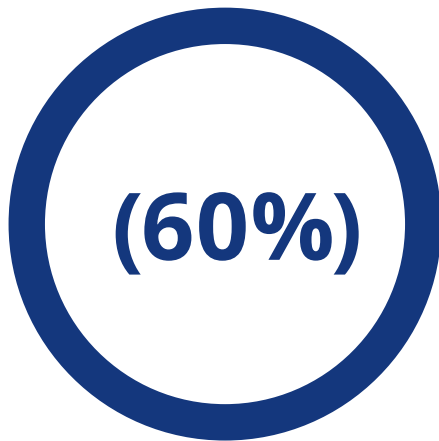
Most organisations had an objective to avoid legal & contractual liabilities, fines⁷ & penalties (62%), or to get a competitive advantage (60%).

It was no surprise to note that most of the organisations considered administrative fines⁵ as the reason to be GDPR ready. However, it was encouraging to note that many organisations considered GDPR as a value proposition for brand and an enabler for competitive advantage.

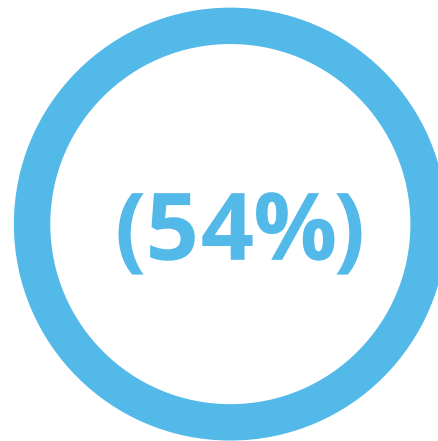
⁷. Administrative fines:

- Fine of up to €10m or 2% of the controller's annual worldwide turnover of the preceding year in case of failure to obtain parental consent where personal data are collected about a child in the process of providing an information society service,
- Fine of up to €20m or 4% of the controller's annual worldwide turnover of the preceding year in case of failure to provide adequate information to data subjects or to allow subject access, or to comply with the right to erasure (amongst others).

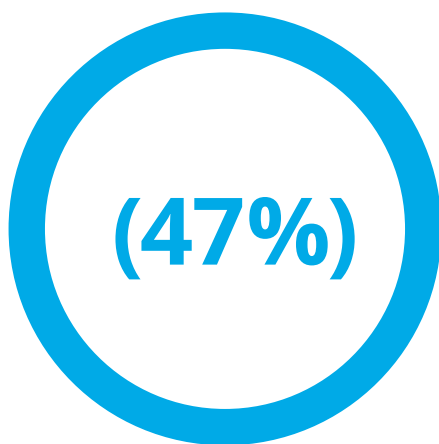
Organisations that are GDPR ready will **gain a competitive advantage** as they will be able to use personal data in their innovations and digitization to provide a better delivery to their clients through the following measures:



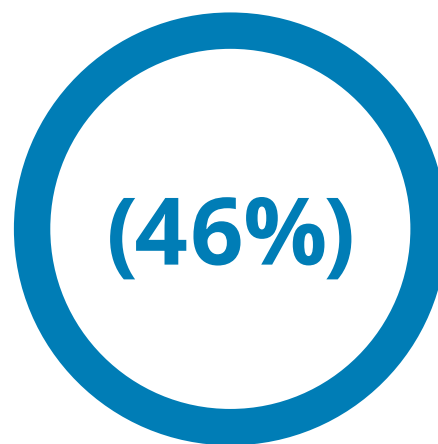
Provide better customer experiences



Enhance productivity of internal operations



Personalization of product & service deliveries



Creation of new products and services



To conclude, organizations have a variety of reasons to be GDPR ready. The results indicate that most organizations view GDPR beyond its regulatory requirement and regard this preparedness as an advantage to provide better customer experiences. The next chapter highlights various strategies adopted by an organization to be GDPR ready.



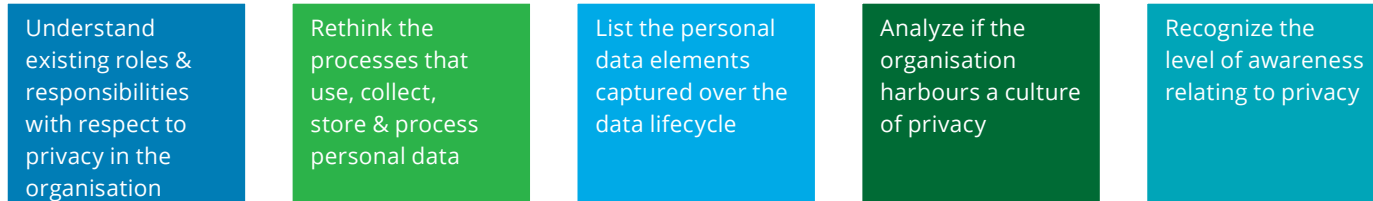


05

Strategy and Governance

Once organisations decide to undergo the readiness journey, it is recommended to follow a structured approach aligned with industry practices. Amongst many aspects of a structured approach, this chapter details the aspects related to awareness, accountability, privacy teams, and designated roles.

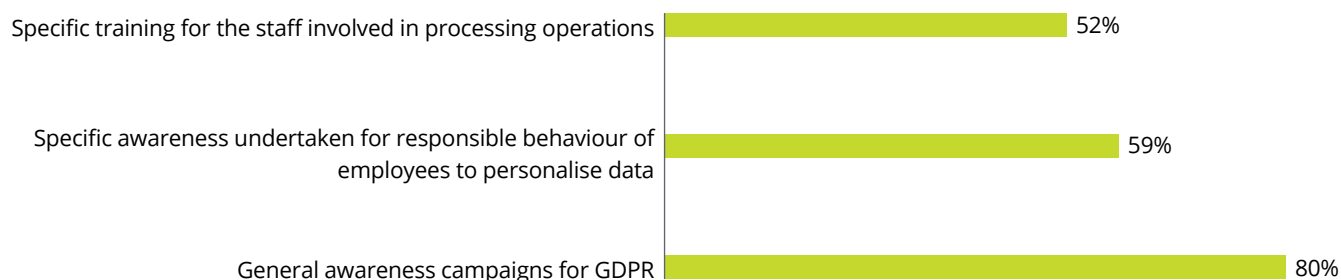
Few of the leading practises followed by organisations are:



Survey results indicate that ~72% organisations have taken steps towards privacy awareness and training requirements of GDPR and ~80% of such organisations recognized “General awareness campaigns for GDPR” as a step taken to spread awareness.

6. Awareness & training requirements

Steps taken towards GDPR



Most of the Indian organisations conduct general awareness campaigns as their key step for GDPR readiness



**Survey
result**

Out of the organisations that have taken action for GDPR readiness, 80% have conducted general awareness campaigns for all their relevant stakeholders to identify their processes which access personal or sensitive data. This will help them streamline their efforts towards GDPR readiness.

Indian organisations must conduct programs for its employees to spread awareness regarding GDPR and its associated privacy practices. It is recommended to build a culture of privacy in every organisation. GDPR emphasizes not only on privacy culture but also on accountability and demonstration. Certain ways of inculcating privacy within an organisation's culture are discussed briefly below.

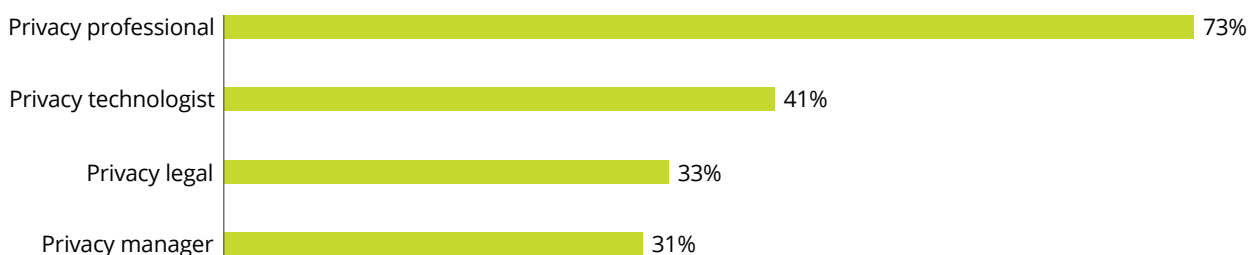
Every employee, especially in the department of personal data processing, must have knowledge of the rules and restrictions with regard to handling personal and sensitive data. Organisations must conduct workshops for employees and subcontractors to build awareness of the rules and regulations regarding GDPR.

Since people play a very vital role in successful implementation of privacy and data protection strategies, it is necessary to have a strong Privacy team to drive the privacy culture in an organisation. While there are no specific requirements for any professional to assess and ascertain the state of GDPR readiness of an organisation, people do take up certain certifications to become privacy professionals (someone who can make decisions, understand business priorities and limitations, deliver training, assist with risk assessment and project management), privacy technologists (someone who incorporates privacy into early stages of IT products and services for cost control, and accuracy), privacy managers (someone who creates organisation's vision and structure

for their privacy team. He/she also develops and implements a privacy program framework.), etc. The basic view of a wide consensus of people in the survey is depicted below.

7. Preferences for privacy team

Most preferred personnels for privacy team



Privacy professionals are preferred by majority of the Indian organisations for their privacy team



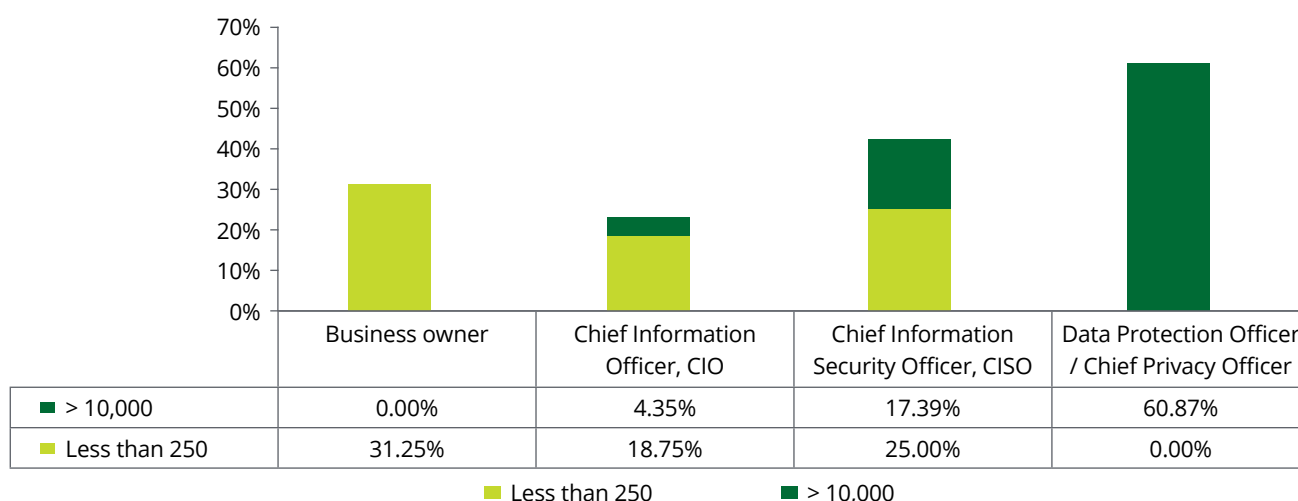
Survey result

73% of our respondents were inclined for a privacy professional to be added to their privacy team for GDPR readiness.

Considering numerous challenges that organisations are experiencing with GDPR readiness, compliance and demand for DPOs, organisations should prioritize training and hiring the right privacy individuals to manage and implement the requirements of GDPR.

The survey suggests that organisations identified specific role to drive GDPR readiness journey. The top-rated roles accountable / designated for the GDPR compliance were Data Protection Officer or / Chief Privacy Officer (responsible for the vision, strategy, and program regarding use of personal information) (~32%) and Chief Information Security Officer (responsible for the vision, strategy, and program to ensure protection of information assets, and technologies) (~ 20%). It was also noted that the majority of small organisations identified their Business Owner or Chief Information Officer as the person-in-charge.

8. Responsibility for ensuring GDPR compliance in the organisation



Most Indian Small & Medium Enterprises have Business Owners in charge of compliance whereas large Indian organisations hand over the responsibility to the Chief Privacy Officer



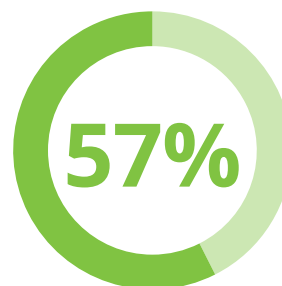
Survey result

Majority SMEs kept their business owner or Chief Information Officer as the person in-charge whereas large enterprises / or organisations preferred a separate Data Protection Officer (DPO) as the head of their privacy team. One of the key reasons to appoint a DPO is regular and systematic monitoring of data on a large scale or processing sensitive personal data on a large scale as "core activities".

Since the responsibility of driving compliance in an organisation cannot reside with one individual, organisations have been increasing and expanding their privacy teams in order to deal with the ever increasing privacy laws and requirements. Key management in addition to HR, Legal, Marketing and security needs to be involved. Organisation's senior employees, must work together to ensure a smooth path to achieving compliance. Organisations cannot be fully compliant without board involvement.

Further, it was noted that the size of a privacy team was relative to the size of the organisation. Privacy teams within an organisation are tasked with data governance, data lifecycle management, etc. and will be continuously challenged to provide clearer, more proactive oversight on data storage, journeys, lineage and other requirements of GDPR. Hence the size of the Privacy team should be substantial in comparison with the size of the organisation.

9. Requirement of a dedicated privacy team



Have a dedicated privacy team

Increased privacy laws and requirements will require organisations to create dedicated privacy teams.



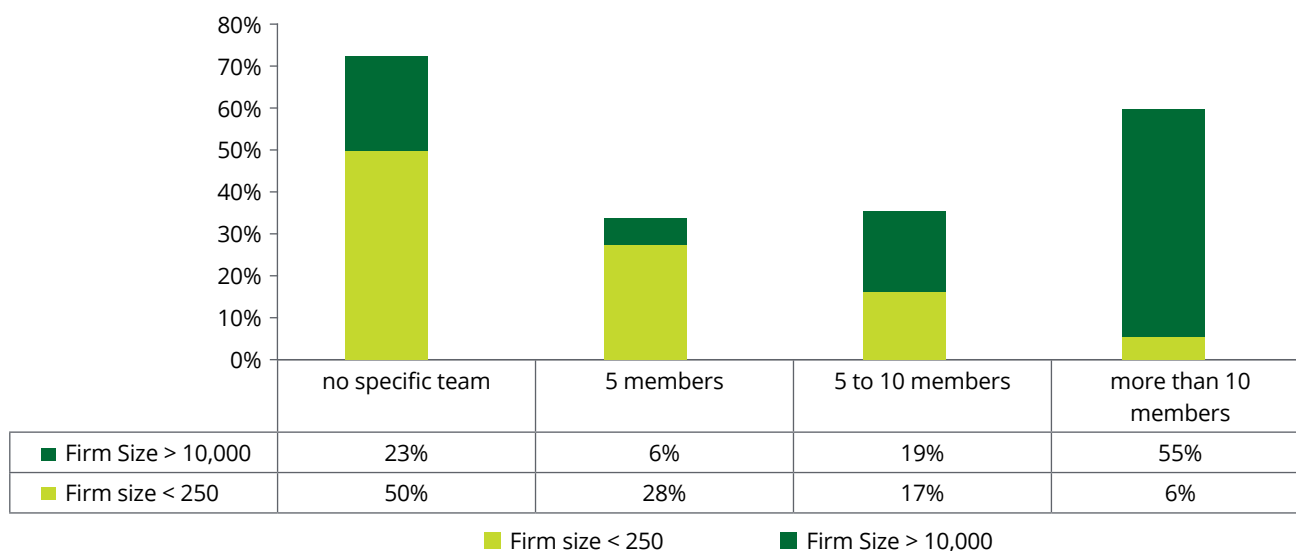
Survey
result

The survey results point out that 57% of the organisations have a dedicated privacy team.

The absence of a dedicated privacy team may pose as a problem for organisations with the increasing number of privacy regulations around the world.

10. Size of the privacy team

Organisation size vs Privacy team size



The size of a privacy team of an organisation was found to be directly proportional to the size of the organisation.



Survey
result

55% of large organisations have more than 10 members in their privacy teams.

To conclude, privacy team and dedicated privacy roles play a critical role in GDPR readiness journey. The next chapter provides an insight into the implementation approach adopted by Indian organisations.

06

GDPR implementation for Indian organisations

Implementing GDPR requires a plan in which it is important to know which elements of GDPR are already in place at an organisation and which are not. These are identified by executing gap assessment. The extent of time and effort to put into a gap assessment is largely determined by the level of detail that it requires. A high degree of detail can be obtained by performing deep dives with relevant stakeholders. Deep dives involve significant time and effort, and thus require clear scoping and co-ordination. The scoping required is determined based on the structure of the organisation and the expected current state of privacy adherence.

The EU GDPR mainly focuses on the personal data of EU/EEA data subjects. Hence it is important to understand all the ways in which an organisation can collect Personal Data⁸ and Sensitive Data⁹.

Survey results identified **leading sectors in India that collect personal data.**

Online Identifier	Directly identifying data	Location Data
Telecom (55%)	Retail (71%)	IT/BPM (38%)
BFSI (52%)	Pharma (64%)	Oil (33%)
Media (50%)	Health (62%)	Internet Service (31%)

This table is indicative of the fact that personal data collection is not limited to a few sectors. This broadly suggests how an organisation comes under the applicability of GDPR as it collects personal data in some way or the other.

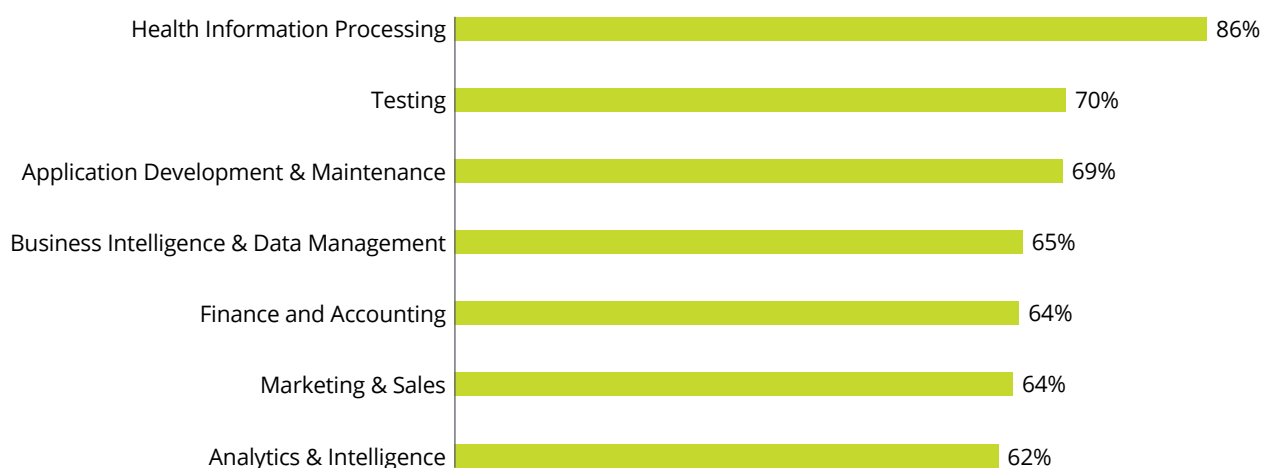
- Online identifiers are collected by telecom companies in the form of IP addresses as they provide web

services, and by the media sector through cookies on their websites.

- Directly identifying data is collected in retail, pharmaceutical and health industries where collecting transactional information is imperative to understand, target and service clients.
- Location data is collected more frequently than ever by many mobile applications that provide region specific services based on the GPS location. Also, applications which are not directly using the location data for their services also collect personal data to provide a better customized experience for every user.

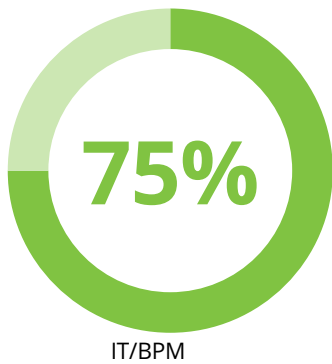
The grounds for processing sensitive personal data are more stringent than the ones for personal data. Below are the lines of services within participating organisations that process sensitive data:

Lines of services dealing with sensitive data

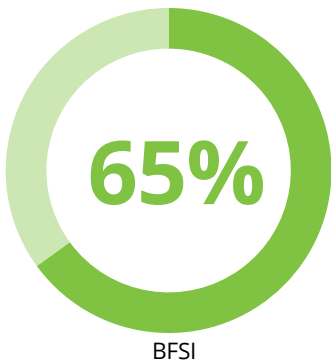


⁸ Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

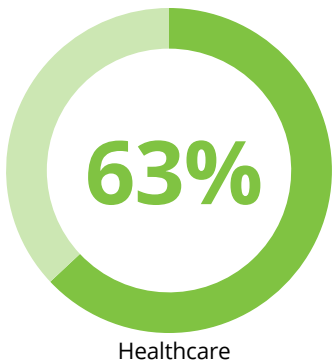
⁹ Sensitive data, referred to as special categories of personal data under GDPR, manifests in the form of data revealing racial/ethnic origin, data revealing political opinion, data revealing religious or philosophical beliefs, data revealing trade union membership, biometrics, genetic data, health information, sexual orientation, etc.



IT/BPM



BFSI



Healthcare

During the survey discussion, it was noted that ‘health information processing’ service line deals with the most sensitive data, containing fields such as genetic data, biometrics, health information, and sexual orientation which can be traced back to a natural person. Similarly, other organisations offering services such as ‘testing’, ‘application development and maintenance’, etc. also extensively indulge in processing of personal data as processors to various EU

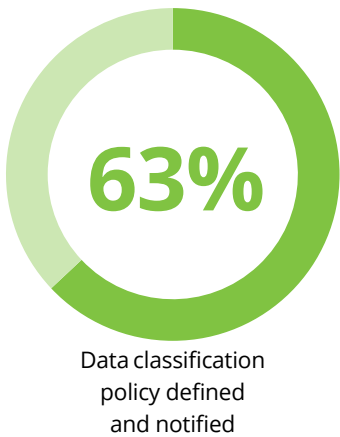
organisations (data controllers) to provide business solutions.

As per the survey results, **leading sectors in India that collect and/or process sensitive personal data** are the IT/BPM, BFSI and Health care sectors. Majority of sensitive data resides in the form of biometrics or health data in these sectors.

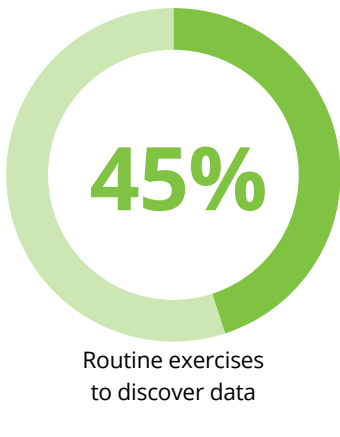
Organizations must have policies and procedures in place to identify the type

of data being collected and the relevant controls required to protect it. At all times, the data lifecycle should be clearly visible to the organisation. Thus, via this survey, organisations were asked about their practices to maintain visibility over personal & special categories of data. The most selected option (~63%) was “Data classification policy has been defined and notified”. Corresponding graph represents the top 3 such leading practices.

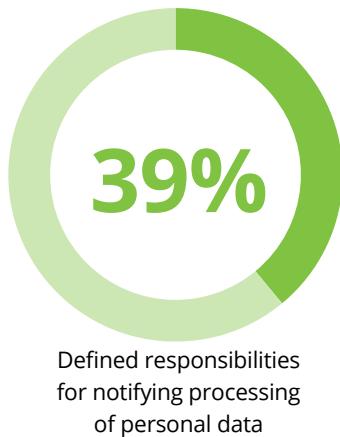
11. Top 3 practices to ensure visibility over personal & special categories of data



Data classification policy defined and notified



Routine exercises to discover data



Defined responsibilities for notifying processing of personal data

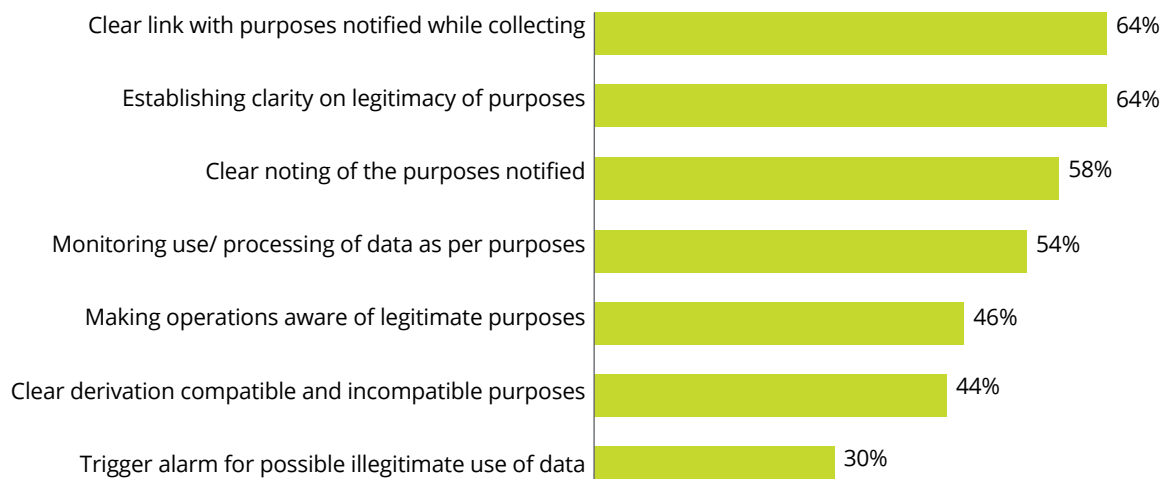
Defining data classification policies and procedures comes out to be the leading practice.

Insight

There should be clear policies and controls in place to provide a clear view of the data lifecycle. Data classification policy enables better indexing, faster access, and quicker recovery times. This policy also helps taking care of redundant, trivial, and obsolete data which in turn reduces the risk. It tells us which data is important and increases awareness regarding its security. It enables the process of data discovery and mapping the flow of data.

12. Best practices for processing personal data

Purpose based data processing



Convey a clear and legitimate purpose for collecting and processing personal data. Use it only for the purpose it was collected.



Survey result

The most prevalent practice seems to be conveying a clear, legitimate purpose for collecting and processing personal data that would link to the intended use of this data. Apart from the aforementioned activity, awareness amongst all operations dealing with personal data, and triggering an alarm when it is being used illegitimately are some of the practices preferred by various organisations across India.

13. Grounds for processing personal data

A closely related requirement is to have legitimate grounds for processing personal data. As per the requirements of GDPR, organisations have to satisfy the following conditions:

Consent of the data subject: Consent has to be clear, unambiguous, freely given, specific and informed. Complying with these qualities will only make the consent legitimate. This also affects the pre-ticked forms which are currently being used by various websites to obtain consent as in this case the consent is not being specifically given but is rather being accepted by the user.

Processing the data is necessary to **protect the vital interests** of a data subject or another person where the data subject is incapable of giving consent. This is probably only applicable in medical emergencies where there are no other grounds available.

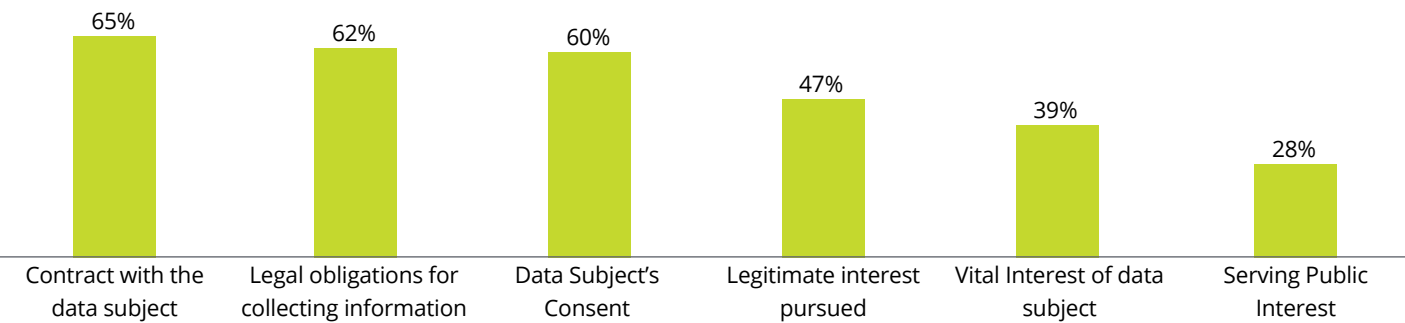
The processing must be necessary for the **performance of a contract** with the data subject or to take steps in preparation for such a contract. This is not a new ground in relation to the old directive. The data should be processed in the scope defined in the contract. Different contractual rules apply to different industries and support functions. The definitions of processing should be concise and not be taken as a generic approach to increase the scope unnecessarily.

The processing must be necessary for the performance of a task carried out in the **public interest or in the exercise of official authority** vested in you under Member State or EU law. It encompasses performing several possible public tasks such as taxes. These are the tasks a public authority has and require personal data processing in accordance with legal obligations. Data processing operations which are seen as being of public interest would be scientific research, public health and more.


The processing must be necessary for **compliance with a legal obligation** of a Member State or EU law to which the organisation is subject. This should be the ground for processing only when the controller has a legal obligation for the processing of personal data.

The processing is necessary for the **purposes of legitimate interests**. What constitutes of legitimate interest is disputed in various lines of services and should be clearly defined

Most preferred grounds for processing



In the Indian context, Contractual agreement is the most preferred ground for processing personal data

**Survey result**

Amongst these conditions to process personal data, the most opted condition (~65%) was “Performance of Contract with the data subject” followed by “Legal obligations demanding collection of information [e.g. KYC]” (~62%) and “Data Subject’s Consent” (~60%).

Insight

An effective consent mechanism must be established with the data subject to gain access for processing his/her personal data.

14. Grounds for obtaining consent

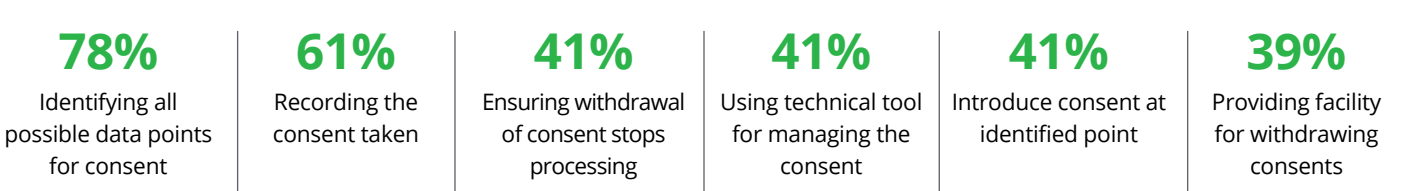
As ‘Data Subject’s Consent’ was selected as one of the top conditions for lawful processing, the respondents were asked about the means of complying with procedural requirements associated with consent. Majority (78%) of the respondents selected “Identifying all possible collection & processing points where consent is required”. Other selections are represented in the graph below.


Conditions regarding how consent should be used for processing personal information have been strengthened. Key considerations include the following:

- Organisations will have to provide a genuine consent;
- The consent must be purpose-limited;
- The terms of consent should be such that the data subject is allowed withdrawal of consent at any given time.

Consent is a widely used ground for processing. This should have a clear form–online or offline, with clear and unambiguous language to convey the purpose and scope of processing the personal data. The terms and conditions should be clearly mentioned and presented in a visible format to the data subject. Obtaining consent can be performed in different ways as summarized later on.

Requirements for obtaining consent



**Survey result**

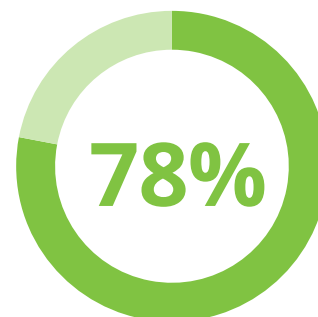
Most Indian organisations felt that identifying all possible data points for consent is crucial.

Insight

The methods for recording consent for all the possible personal data collected is considered as a pivotal step in taking consent for processing personally identifiable information.

Explicit consent for Sensitive data

Sensitive data is a category of personal data for which taking consent explicitly is mandatory as per GDPR guidelines. Explicit consent can be taken through various mediums. Survey results indicate the most prevalent practices followed in the industry to obtain explicit consent.

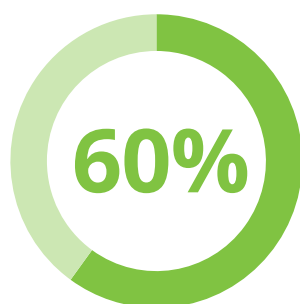


% of organisations dealing with sensitive data are using consent as the grounds

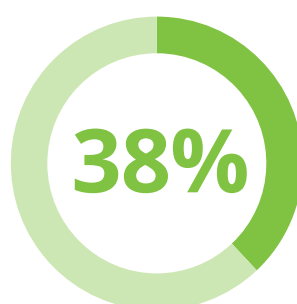
15. Methods for obtaining explicit consent



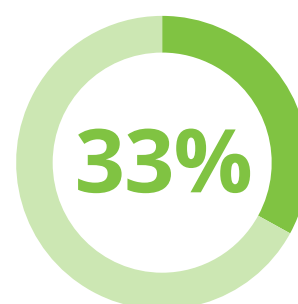
Filling an electronic form



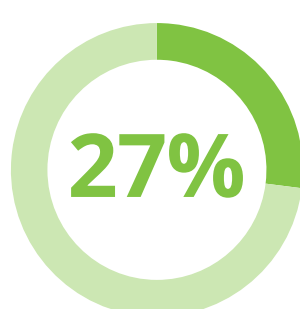
Written form



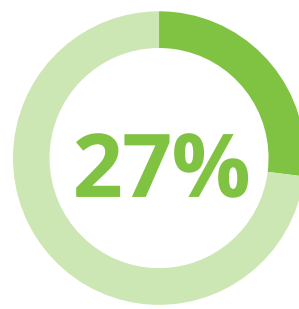
Logging data subjects' actions



Sending an email



Scanned document carrying a signature



Opt-in mechanisms after detailed notice

It was noted that filling electronic and written forms are the most widely used methods to gain explicit consent.



Survey result

While the survey revealed that 78% of the organisations dealing with any type of sensitive data consider 'consent' as their grounds for processing, 69% responded that filling an electronic form is the most widely accepted method of providing consent.

Insight

Organisations found form filling (online or offline) as the most convenient way to obtain explicit consent from data subjects.

The survey results were correlated to identify the industry-wise top rated medium (i.e. written form or electronic form) for obtaining explicit consent. The results indicate that the Pharmaceutical sector and procurement line of business prefer using written forms as their medium of consent justifiably as they are considered to use conventional methods in their business. However, sectors and lines of services like IT and marketing & sales use electronic forms as their consent method because they have adapted and embraced the evolving technologies in their style of functioning.

Used in	Written form	Electronic form
Sector	Pharma (67%)	Internet Services/IT (65%)
Line of business	Procurement (60%)	Marketing & Sales (90%)

The underlying privacy principles for obtaining consent and handling of personal or sensitive personal data are discussed in detail after gaining insights about the industry-wise trends

Privacy principles under GDPR¹⁰

Organisations are required to comply with GDPR by incorporating the following privacy principles in their operations:



¹⁰ Article 5 (principles relating to processing of personal data), European Union's (EU) General Data Protection Regulation (GDPR)

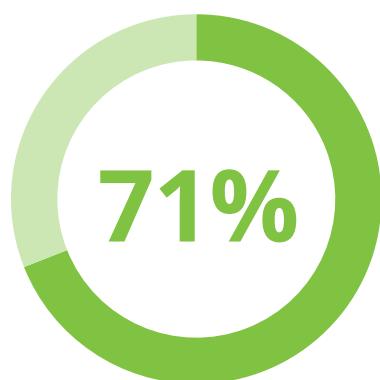
As per the survey results, organisations indicate that Integrity and Confidentiality along with being able to demonstrate accountability would require the most effort for compliance.

Revitalization required for following principles

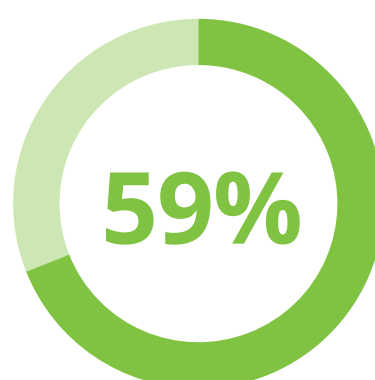


In continuation, participants were asked for views on the impact of rising expectations of the privacy principles enshrined by GDPR. Surprisingly, a majority (71%) of them expressed that it helps in bringing sense of privacy in business and innovation ideas.

16. GDPR privacy principles – boon or bane for Indian organisations



On the contrary, it helps in bringing sense of privacy in business and innovation ideas



Objections to automated processing would limit potential of analytics, ML, and AI



Survey result

71% of respondents believe that, privacy principles will help bring a sense of privacy in business and innovation ideas. They were appreciative of the positive impact these principles will have over their business. Moreover, they are keen to utilize this opportunity to make their organisation more data secure and ahead of their competition.

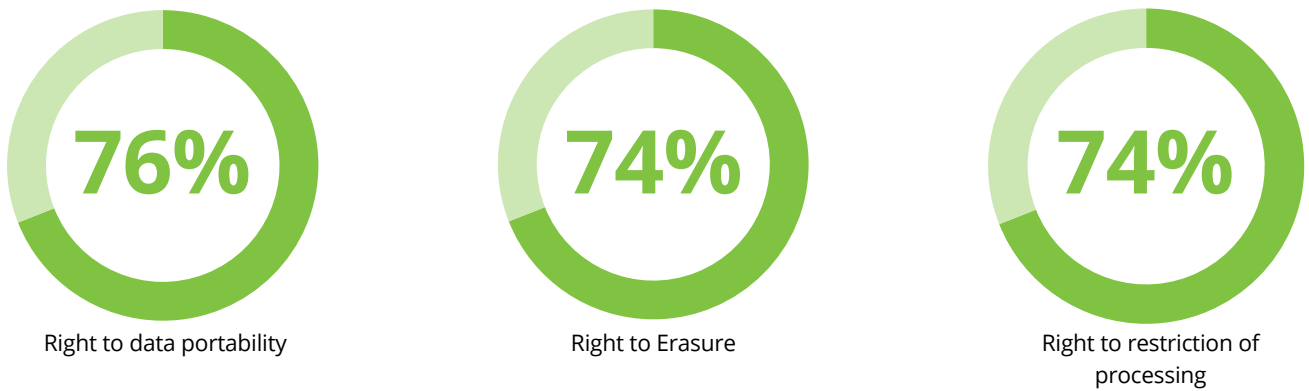
On the other side, they do believe that it will have an impact over the automated processing that is being introduced with the help of Machine Learning (ML) languages and AI.

Insight


Privacy principles prove to be helpful in guiding organisations rather than being a hindrance for their business operations.

After understanding the industry’s view on privacy principles and the level of effort to demonstrate compliance, it was important to understand the challenges in GDPR readiness journey. On questioning about the most challenging ‘data subject right’, participants opted for **“Right to Data Portability”, “Right to Erasure”** and **“Right to Restriction of Processing”** as the top three challenges.

17. Data subject rights



Organisations consider the ‘Right to data portability’ as the most challenging Data subject right.

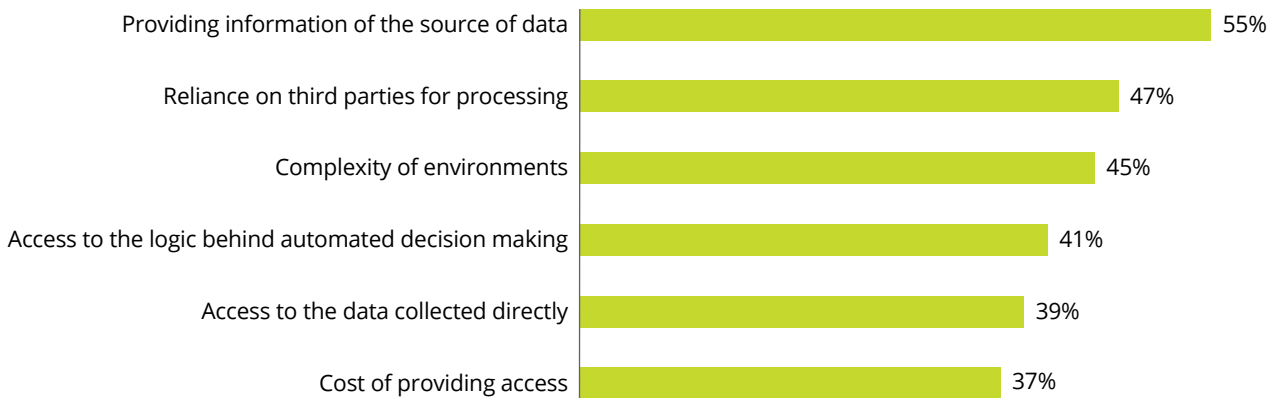
 **Survey result**


‘Right to data portability’ emerged as the most challenging data subject right to implement. ‘Right to erasure’ and ‘Right to restriction of processing’ were rated second and third most challenging right to implement.

Additionally, participants were asked about the challenges to execute these rights. The following representations summarize their responses.

18. Right to data subject access - challenges

Challenges for right to data subject access



 **Survey result**

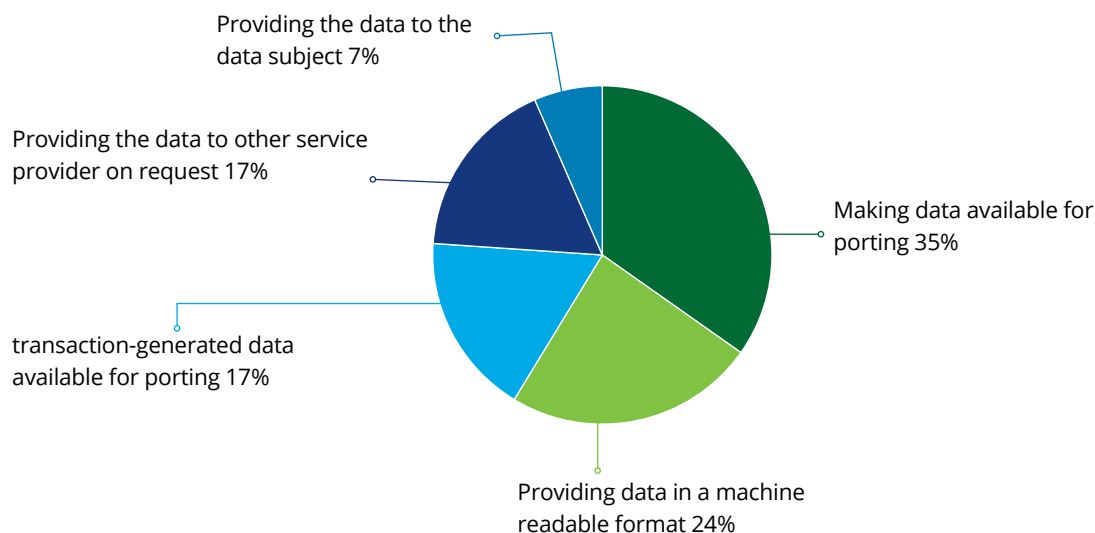
The key challenges faced in providing this right to data subjects are in providing the source of the data (55%) and their reliance on third parties for processing (47%).

Insight

There has to be a clear visibility of data across its lifecycle.

19. Challenges in implementing right to data portability

Challenges for implementing data portability



Survey result

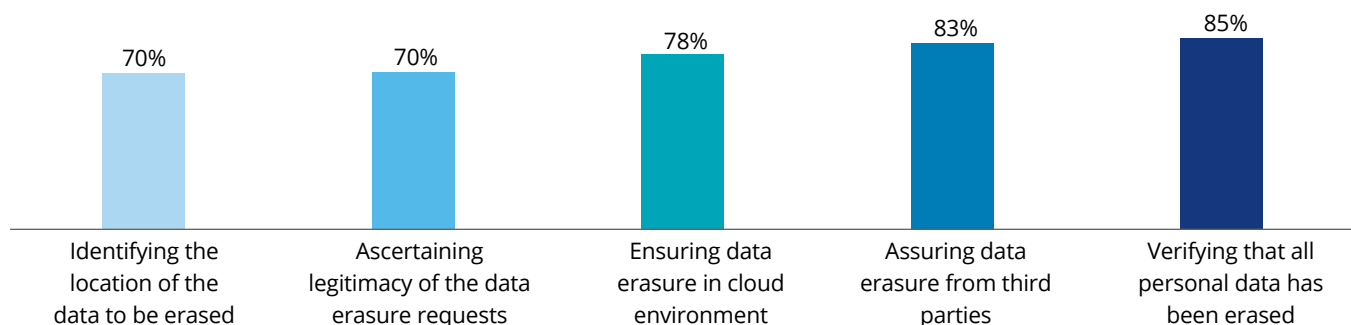
The two main challenges survey respondents feel would be making the data available for porting and providing the data in a machine readable format. From this result, it may be inferred that most organisations do not follow a standard format for storing data—each follow their own format according to their requirements. This results in the problem of restructuring old stored data to make it portable.

Insight

Common formats should be considered by organisations to make data portability easier.

20. Challenges for right to erasure

Challenges for right to erasure



Survey result

Assurance of erasure of data from third parties and verification of its erasure are the most crucial concerns.

Insight

There has to be a clear visibility of data across its lifecycle.

To conclude, processing of personal data as per the requirements of GDPR will not only help organisations conduct business with ease in the EU and EEA, but also help their customers, vendors and suppliers consider them as trustworthy. The next chapter provides a view on how organisations are preparing their extended teams (vendors, contractors, etc.) for GDPR readiness.



07

Maintaining concurrence with GDPR

Implementation of GDPR in an organisation is not a one-time activity but a constant process which has to be embedded in the culture of the organisation to face any challenges that might arise in the future. According to chapter 4 (controller and processor) of GDPR, there are certain obligations that have to be abided by the controllers and processors. These obligations are fulfilled by implementing appropriate technical and organisational measures to comply with the procedural requirements of GDPR. A controller should use only those processors who comply with the requirements, and the engagement between them has to be governed by a contract. The contract contains the subject-matter and the duration of the processing. Other requirements should also be mentioned in the contract such as record keeping activities, data protection impact assessment (DPIA), etc.

With the enforcement of GDPR, many organisations will have to revise these contracts to reflect upon the new arrangements of liability sharing and the clauses within these contracts.

Prior to GDPR, contracts that were signed between organisations regarding processing and sharing the liability were not mandatory. From the results, a change is foreseen regarding this scenario as more and more organisations will now have comprehensive discussions on the sharing of liability. A blanket policy is a policy which covers a plethora of liabilities. With GDPR enforcement, it is likely that the conditions that come under blanket policies will be pushed by the clients to increase liabilities on service organisations.

The requirements and obligations to be fulfilled with respect to GDPR are covered in the sections below.

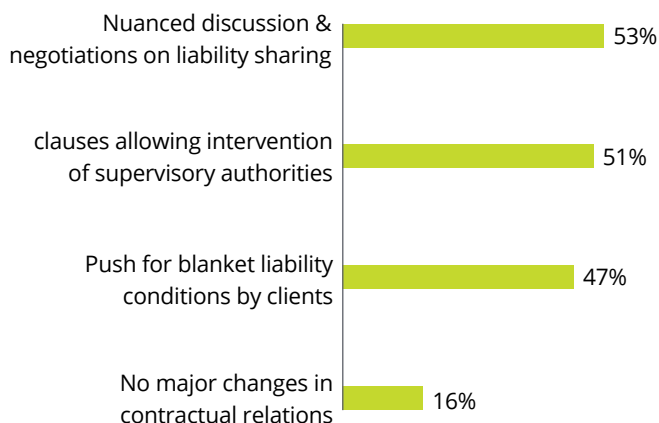
Records of processing

As per Article 30, GDPR expects organisations to maintain records of all processing activities involving personal data.

Any organisation irrespective of its size is expected to adhere to this requirement if they handle vast amounts of personal data or special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences as per Article 10. According to the survey results, organisations with less than 250 employees strongly believe that they have central visibility over all processing activities and so this requirement (records of processing) does not apply. Organisations with more than 10,000 employees believe that policies and format for maintaining records is an important step for them.

Changes foreseen in the contracts due to GDPR

Changes foreseen in GDPR contracts



Steps taken for record keeping

Firm size < 250	Central visibility over all processing activities (47%)	This requirement is not applicable to my organisation (27%)
Firm Size > 10,000	Organisational policy, guidance & format for maintaining record of the processing activities (58%)	Obligation on business operations to inform the processing of data (47%)



Privacy by design

The standardized and repeatable process of privacy by design and by default ensures that the organisations understand the appropriate privacy and data protection controls as a project begins, rather than only considering privacy as a checkbox exercise. This enables not only privacy and data protection teams, but also security teams to help provide advice, guidance, and review the process from the beginning itself.

Security of Processing

Taking into account the sensitivity of the personal data processed, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks involved:

- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

The controller and the processor must also take steps to ensure that any person who has access to personal data under their authority does not process it unless required by the law or instructed by them.

Data Lifecycle Management:

Privacy and security risk management intersect with other data lifecycle management programs within an organisation. A good management program must continually assess and review who needs access to what types of information.

- Organize the collected personal data: The data that is stored in the organisation must be in a secure and private place under lock and key. Its access should only be on a need-to-know basis;
- An authorization structure should be in place to prevent misuse of personal data;
- There must be deletion and retention rules in place for the collected data that no longer serves the processing purpose.

Data Protection Impact Assessment (DPIA):

DPIA should be conducted as soon as a new technology comes into effect, so as to incorporate the measures identified by it, into the updated policies of the organisation. In order to enhance compliance with the GDPR where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for carrying out a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk.

It should be conducted as soon as a new technology comes into effect, so as to incorporate the measures identified by it, into the updated policies of the organisation.

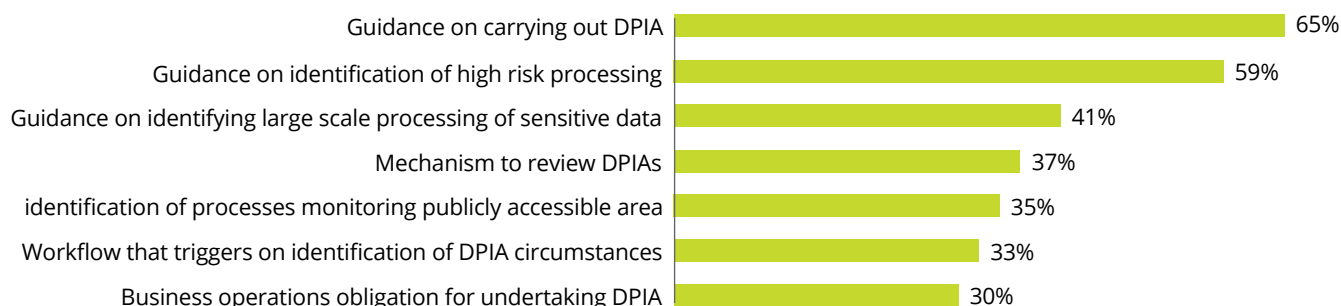
In such cases, the controller of an organisations needs to define the circumstances under which a DPIA is to be conducted. That impact assessment should include the measures, safeguards and mechanisms envisaged for mitigating the risks, ensuring the protection of personal data and demonstrating compliance with GDPR.

A DPIA is especially required in the following cases:

- A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- Processing of personal data on a large scale of natural persons or processing of data related to criminal convictions and offences;
- A systematic monitoring of a publicly accessible area on a large scale.

21. Data protection impact assessment (DPIA)

Steps taken towards DPIA



65% organisations issued internal guidance to conduct the Data Protection Impact Assessment.

Insight

DPIAs help organisations identify, assess, and mitigate or minimize privacy risks with data processing activities. They are particularly relevant when a new data processing process, system, or technology are being introduced.

The guidance issued by organisations include assessment measures and procedures. DPIA assesses the following:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- The necessity and proportionality of the processing operations in relation to the purposes;
- The data protection risks and risks related to the rights and freedom of the data subjects (impact on data subjects);
- The measures that will address the risks to the rights and freedom of the data subjects along with issues such as cross border transfers.

The DPIA is not mandatory when the processing of personal data is not on a large scale, for instance, the possession of personal data of patients and clients by an individual physician.

DPIA also identifies the data protection solutions that will mitigate the risks. The decisions taken after the assessment should be documented as part of the DPIA process. Where necessary, the controller will carry out to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

As per the survey, the support that organisations require for conducting DPIA are as below:

Steps taken for DPIA	
Controller	Business Operations obligation for undertaking DPIA on requires circumstances (55%)
Processor	Guidance on identification of high risk processing (74%)

Appointing a Data Protection Officer (DPO)

To effectively perform the duty of maintaining the privacy function of an organisation, large corporations, government

bodies, organisations in the health and social care sectors, financial institutions, and most organisations based in the EU will have to appoint a Data Protection Officer (DPO) who would be responsible for formulating data protection strategy and make the organisation compliant with GDPR requirements.

GDPR names three entities involved in the processing of data, i.e. the controller, processor and third parties. The main task of the DPO would be to work closely with these data processing entities and ensure their compliance with the GDPR requirements.

He/she also should play a passive role in data protection by

GDPR actively lays down task of DPO which is:

- 01 To inform and advise the controller and the processor of their obligations to the Regulation
- 02 To monitor compliance with the regulation
- 03 To provide advice where requested about data protection
- 04 To cooperate with the supervisory authority

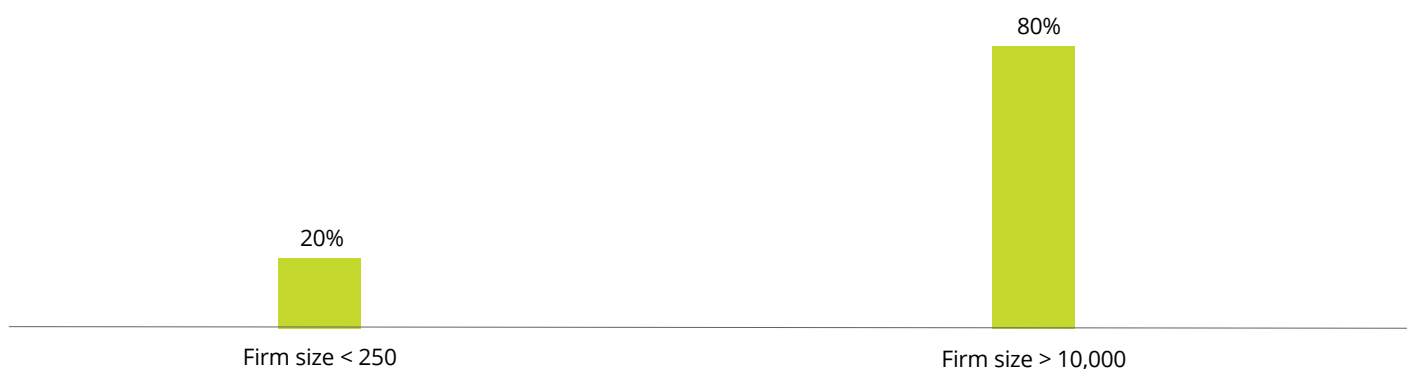
training staff and raising awareness on data protection. For further details, refer to 'guidelines on Data Protection Officers'¹¹ as released on 13 December 2016.

Cases for appointment of a DPO are mentioned below:

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- The core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale;
- The core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

22. DPO appointment

Firm size vs. DPO appointment



80% of large Indian firms chose to appoint a DPO, on the other hand, only 20% of Small & Medium Enterprises (SMEs) appointed a DPO

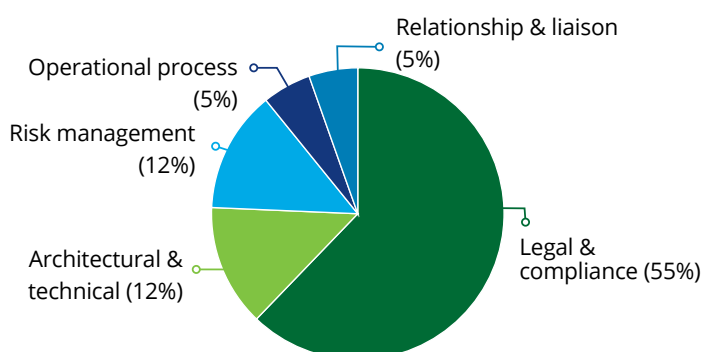
Insight

Large Indian firms appointed a DPO proactively as a part of their readiness activities as compared to Indian SMEs.

Talking about the qualifications of DPO, the degree of sensitivity of data that an organisation is holding and processing should be directly proportionate to the expertise and skills of the DPO that they appoint. He should be able to fulfil his duties which are required out of him.

23. Preferred skill sets for DPO in india

Skills preferred in a DPO



55% of Indian organisations indicate legal & compliance as their most preferred skill set while appointing a DPO



Survey
result

Legal & Compliance is the most preferred skill set for DPO in India.

Insight

Organisations are inclined to appoint DPOs who have a background on the Legal and Compliance requirements.

¹¹. 'Guidelines on Data Protection Officers'. (2016) .Available at : http://ec.europa.eu/newsroom/document.cfm?doc_id=43823

Data Breach Notification

A personal data breach is when there is an unauthorised disclosure of sensitive data to an untrusted environment. A personal data breach might, if not addressed in an appropriate and timely manner, may result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, etc.

In compliance with GDPR, the data controller must, without delay, notify the authorities of the said data breach, unless the personal data breach poses no threat to the rights of the data subjects. A delay of 72 hours or less is feasible, extending which will require the controller to submit a detailed report to the Supervisory Authority, clearly stating the reasons for delay.

It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject.

The breach notification that is to be submitted will include the following:

- A detailed assessment of the nature of the breach, along with the extent of damage to the rights of the data subjects;
- The contact details of the DPO;
- The consequences of the breach;
- Proposal of the remedial actions to be taken so as to mitigate the damage.

The controller will also have to communicate the breach notification to the data subject in case the breach threatens the privacy and security of the latter. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities.

24. Steps taken by controller vs processor for data breach notification

Steps taken for Data Breach Notification		
Controller	Have a procedure in place to notify the supervisory authority within 72 hours of becoming aware of a breach (60 %)	Technical and procedural arrangement to detect data breach (63%)
Processor		Procedure and obligations for reporting the instances/ breaches by business operations (45%)

60% of the Controllers and processors have a procedure in place to notify the supervisory authority within 72 hours of becoming aware of a breach.



Survey result

The survey results reveal a similarity in the steps taken by controllers and processors w.r.t. a procedure in place to notify the supervisory authority within 72 hours of becoming aware of a breach. Under the regulation, a controller needs to notify about any breach as early as possible. However, a Data processor must have an internal breach notification process to identify and notify the same to the Data controller when detected.

Insight

The difference observed was that controllers are more focused towards the technical and procedural arrangement as they have to detect a data breach for notification. The setup for observing these breaches becomes of essence as controllers maintain a vast database of their data subjects. Processors, on the other hand, are more concerned about the reporting procedure for these data breaches. Since they have the obligation of notifying the supervisory authority within 72 hours of becoming aware of data breach, reporting becomes an important executable exercise for them.



08

Data transfer between India and EU

In today's global and digital age, cross border data transfers drive growth and stimulate innovation. Indian IT Industry exports today amount to \$120bn each year and about 30% of these exports can be attributed to the EU market where GDPR implies. These exports can be seen as the result of huge amounts of exchange of crucial data due to processing needs of the EU organisations. But this exchange of data can also lead to privacy and protection related risks for both the parties involved.

The European Commission has set up legal obligations to be fulfilled for personal data transfer of EU data subjects to third countries (countries not present in European Economic Area). Third countries that have an adequacy decision in favour by

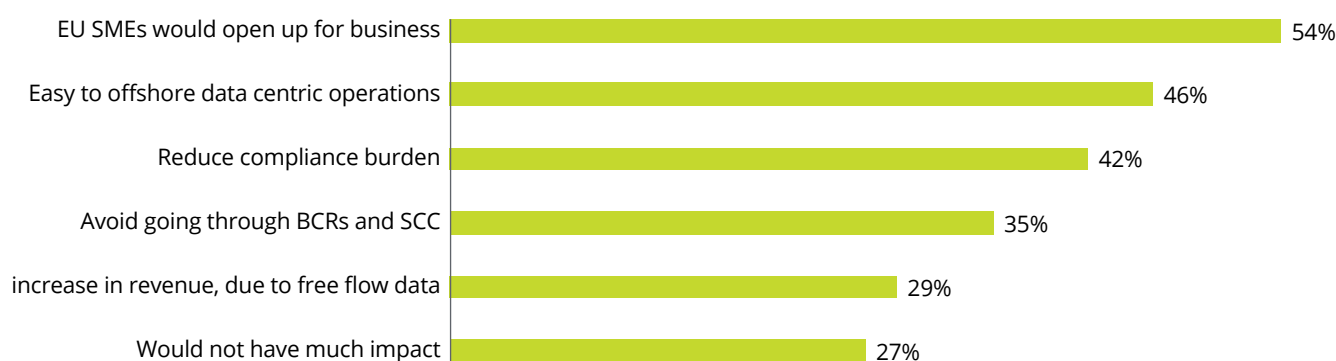
the European Commission can have cross border data transfer with the EU organisations with ease. The adoption of an adequacy decision involve:

- A proposal from the European Commission;
- An opinion of the European Data Protection Board;
- An approval from representatives of the EU countries;
- The adoption of the decision by the European Commissioner.

Benefits of adequacy

The benefits of acquiring a adequacy status are as shown below:

Adequacy Status Benefits



Adequate countries become centres for data processing operations as the facilitation of data transfer between organisations is done in a smooth manner while complying with all the rules and regulations.

25. Opportunity vs Compliance

Benefits seen by small and large firms from adequacy status

Firm size <250	Small & mid-size EU companies would open up for the business possibilities (58%)	Easy to offshore data centric operations (43%)
Firm size >10,000		Avoid going through instruments like BCRs and SCC (48%)

SMEs are focusing on the opportunities they would get when they become GDPR ready by having various EU clients engage with them for future projects.



Survey result

58% of the respondents are of the view that small & mid-size EU companies would open up for the business possibilities.

Insight

The scope of business for SMEs will increase because of the ease to offshore data centric operations. On the other hand, large firms are focusing more on the cross border data transfer rules and compliance limitations.

Only a handful of countries have been considered as 'adequate' by the EU (India is not part of this list).

For Indian organisations to facilitate cross border data transfer with entities present in the EU, instruments for cross border data transfer have to be used.

Rules for cross border data transfer lay out two conditions for adequate data storage and processing:

- Personal data can be allowed to transfer to countries that provide adequate level of protection for the personal data that is being exchanged;
- It is the responsibility of the controller to foresee the level of protection of data and provide

safeguards in place wherever the protection is seemingly lower or not adequate for the personal data is being exchanged.

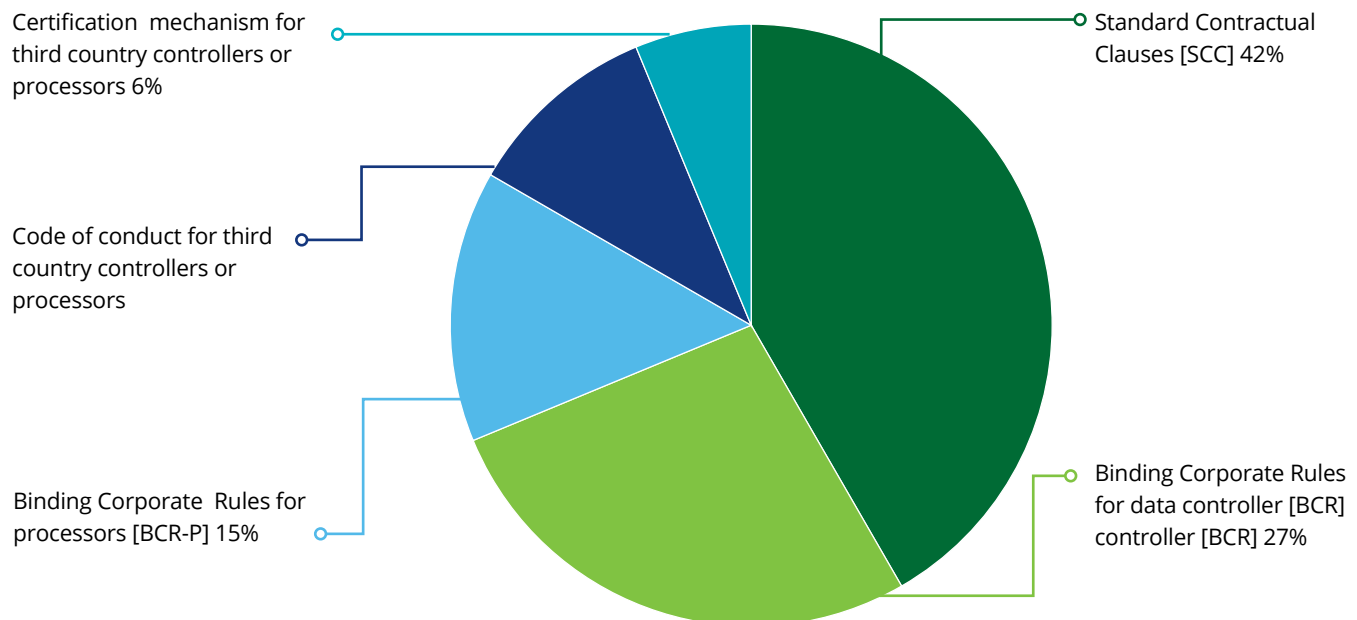
When personal data moves across borders, risk may be increased of the unlawful use or disclosure of this data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among

data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. The Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with GDPR.

There are several instruments used by organisations for cross border data transfer. The pie chart depicts the most widely used instruments by various organisations from the survey results.

26. Most widely used instruments for cross border data transfer

Instruments used for cross border data transfer



Indian organisations mostly use Standard Contractual Clauses as the instrument for Cross Border Data Transfer.



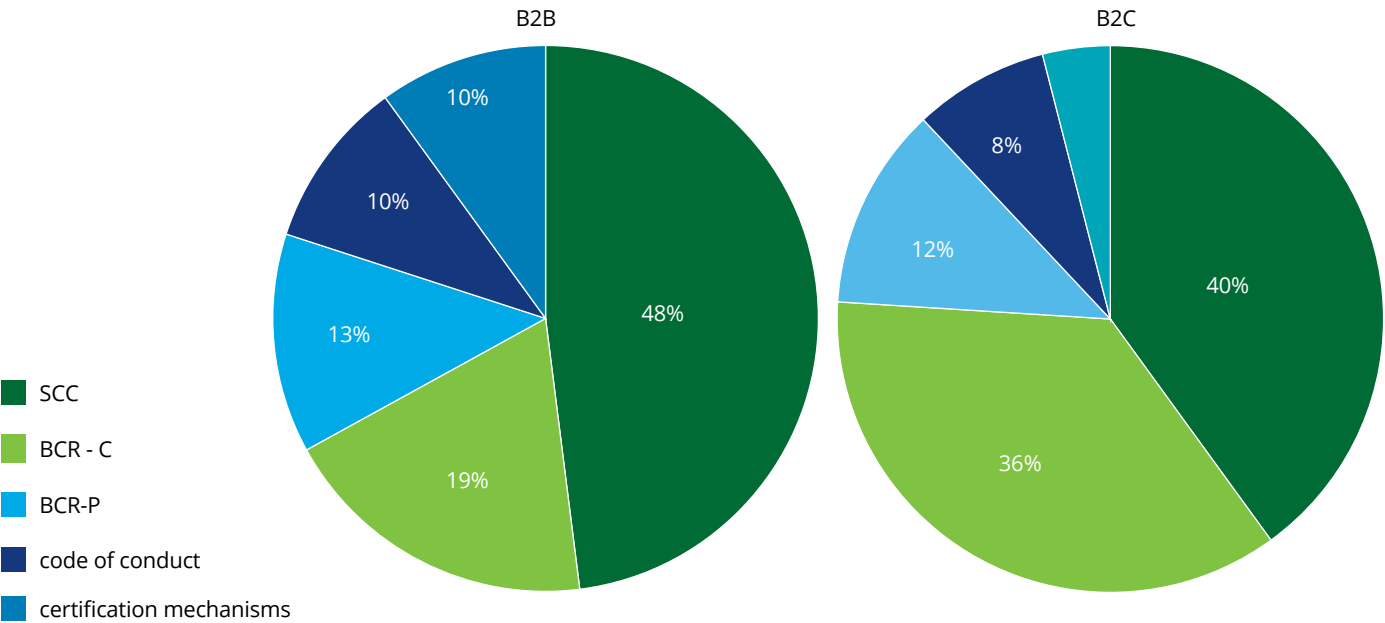
**Survey
result**

43% of Indian organisations mostly use Standard Contractual Clauses as the instrument for Cross Border Data Transfer.

Insight

Standard contractual clauses and Binding Corporate rules are the main instruments referred to for Cross Border Data Transfers.

27. Cross border data transfer instruments used – B2B VS B2C



Almost half of the B2B organisations use Standard Contractual Clauses (SCC) as the instrument of choice. B2C organisations prefer using Binding Corporate Rules and SCC.

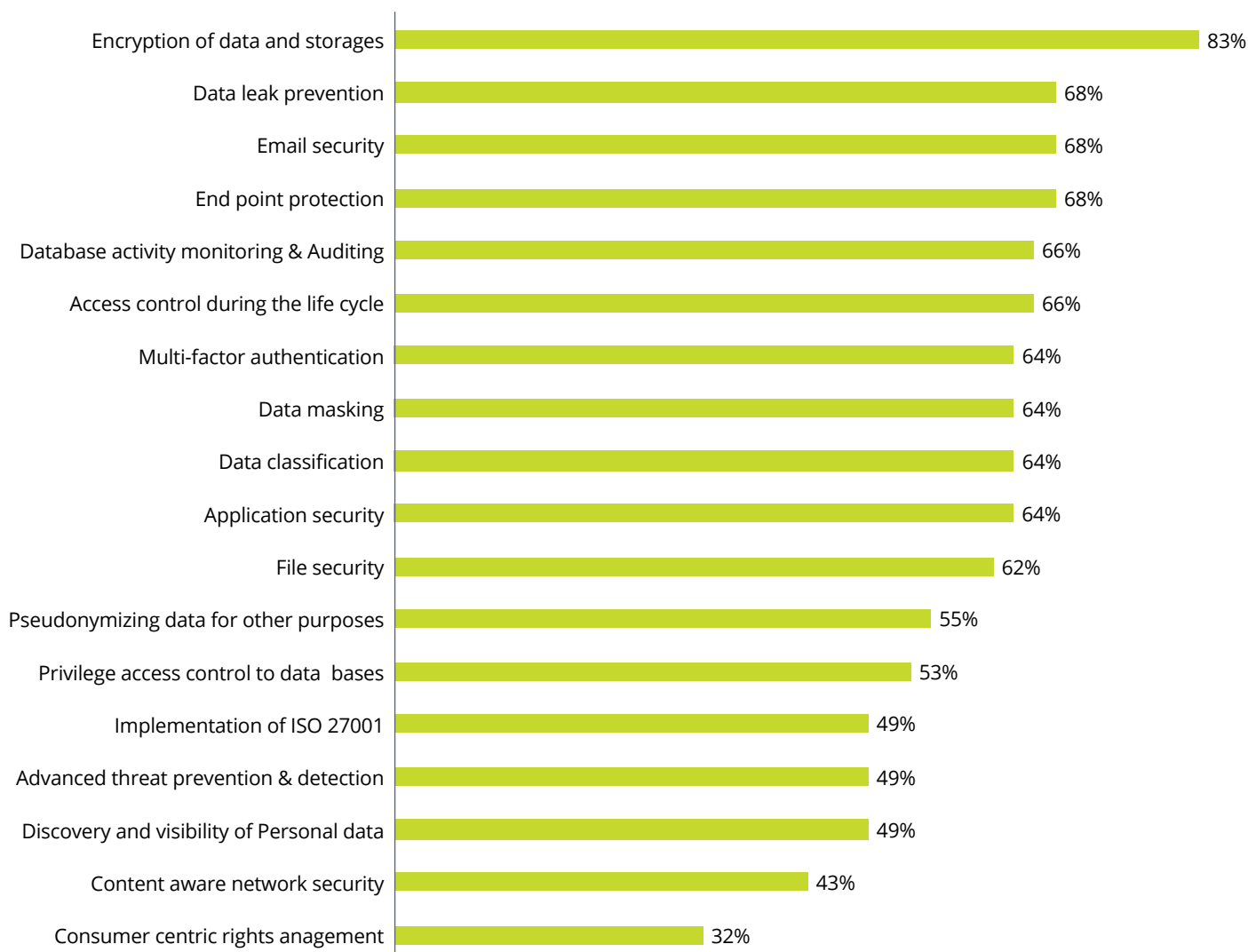
Survey result 48% of the B2B organisations use Standard Contractual Clauses (SCC) as the instrument of choice. B2C organisations prefer using Binding Corporate Rules (BCR) (40%) and SCC (36%).

Insight SCCs are more widely used across Indian Industries. BCRs are picking up pace in customer-centric businesses.

09

State-of-the-art measures

28. Preferred state-of-the-art security measures



Encryption leads the pack of state-of the-art measures because of its wide implementation throughout an organisation's data processing activities.



**Survey
result**

Encryption is leading the pack of state-of the-art measures because of its wide implementation throughout an organisation's data processing procedures.

This is followed by email security as the most crucial data of business processes of an organisation is transferred over mail. These are followed by data centric measures such as database activity, masking, classification, pseudomysation, and discovery.

Consumer centric measures would pick up with time as consumers get more privacy conscious. Hence at the time of the survey, consumer centric measures are not much prioritized.

Insight

The most preferred measure will depend on the business processes of an organisation.

About Deloitte

All the facts and figures that talk to our size and diversity and years of experiences, as notable and important as they may be, are secondary to the truest measure of Deloitte: the impact we make in the world.

So, when people ask, “what’s different about Deloitte?” the answer resides in the many specific examples of where we have helped Deloitte member firm clients, our people, and sections of society to achieve remarkable goals, solve complex problems or make meaningful progress. Deeper still, it’s in the beliefs, behaviors and fundamental sense of purpose that underpin all that we do.

Deloitte Globally has grown in scale and diversity—more than 263,900 people in 150 countries, providing multidisciplinary services yet our shared culture remains the same.

About DSCI

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, Law Enforcement Agencies, Industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Acknowledgements

The GDPR Preparedness Survey Report is the result of the efforts of the Deloitte Risk Advisory and DSCI Project Team. The report has been shaped by the responses and experience of practitioners from more than 50 organizations across industries. The team at Deloitte and DSCI has worked tirelessly to integrate the multiple facets associated to GDPR and its implications on India. We'd like to acknowledge the undeterred support of our team members –

Kartikeya Raman, for the overall management of the survey and report. We appreciate your focus, effort and perspectives put forth in this report.

Ambika Bahadur and Himanshu Pathak from Deloitte and Amit Ghosh, Priti Vandana and Anand Krishnan from DSCI, for leading the survey efforts and engaging in meaningful discussions to shape this report.

Rati Acharya, for managing all the many details involved in this complex undertaking.

Sanya Kalani and Udit Jain, for weaving together this report with their creative insights.

Contacts

**Rohit Mahajan**

President
Risk Advisory
rmahajan@deloitte.com

Rama Vedashree

CEO
DSCI
rama.vedashree@dsci.in

Shree Parthasarathy

Partner
Risk Advisory
sparthasarathy@deloitte.com

Vinayak Godse

Senior Director
DSCI
vinayak.godse@dsci.in

Vishal Jain

Partner
Risk Advisory
jainvishal@deloitte.com

Gautam Kapoor

Partner
Risk Advisory
gkapoor@deloitte.com

Manish Sehgal

Partner
Risk Advisory
masehgal@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 and the information contained herein prepared by Deloitte Touche Tohmatsu India LLP ("DTTILLP"), is intended to provide general information on a particular subject or subjects and is not an exhaustive treatments of such subject(s). None of the DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by any means of this material, rendering professional advice or services. The 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 who relies on this material.