

Current Issues in Retirement Benefits

Mumbai

September 6, 2019

Data Privacy Demands in Employee Benefits Valuation

Inderjot Kaur Dang

Chief Risk and Compliance Officer, Mercer India and GOSS



Agenda



The Need of Data Privacy?



Obligations to protect data – Why?



Breaches



Consequences of breaches



Our Responsibilities



Competitive Advantage

The Need Of Data Privacy?



Employee Benefit actuaries frequently work with sensitive data such as compensation histories, retirement benefits etc.



Actuaries invariably receive Personal Information (PI) such as names and dates of birth and hire, Social Security numbers and home addresses



The risks—both for the individuals whose data is entrusted to us, and for our clients/employers—are too great for actuaries not to take privacy very seriously



Employee data used responsibly can benefit everyone within an organization; however, misused information can lead to violations of privacy laws/regulations and internal Company policies

Obligations to Protect Data – Why?



The Actuary will be under certain obligations in how they deal with Personal information and protect data.

Actuaries must be aware of their privacy obligations under applicable laws and take those obligations seriously.



TRUST OF CLIENTS

Our clients and their employees, our business partners and our colleagues around the world entrust us with their Personal Information as well as confidential business data



CODE OF CONDUCT

Actuarial Professionals to adhere to their Professional Code of Conduct across the World. Violation of Code may lead to relevant actions



LEGAL OBLIGATIONS

Laws, Regulations around the world requires Companies, employees and professionals to comply with legal provisions for the protection of Data. Violations may lead to huge penalties, imprisonment etc.

Obligations to Protect Data – Why?



No Trust means No Business

The goal of companies is to offer trustful services to their clients. In return, Clients trust Companies with sensitive information, personal information. Whilst, no business intends to harm their clients, an unintentional or accidental data leak could potentially impact your business reputation.

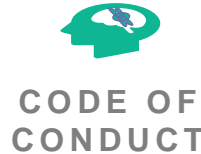


Companies are contractually obligated with Clients to comply with the clauses w.r.t. the protection of client data, personal information and confidential information. Violation of contractual obligation can have financial liability, litigation cost.



Obligation to protect data about Third Parties received from the Client. Third party data may include personal data about third parties such as insurance or pension policy holders.

Obligations to Protect Data – Why?



Actuary Members need to comply with data protection obligations as per the applicable Code of Conduct around the world.



India

The Professional Conduct Standards (PCS) gives guidance on professional conduct in addition to that is provided under the Act and Rules & Regulations made thereunder and Other Guidance to which all members must conform in both the spirit and the letter.

PCS mandates that CI should not be disclosed unless consent has been obtained from the Actuary's client or the Actuary's firm, as the case may be.

Seek legal advice before disclosing CI, if required either by virtue of statutory or judicial authority or by virtue of other guidance by which the client is bound or in public interest.



United Kingdom

The Actuaries' Code Principle 1 – Integrity requires Members to respect “Confidentiality”.

Users and the general public are entitled to expect that sensitive information will not be misused, treated carelessly or, other than in exceptional circumstances, be shared without permission.

In the absence of a user's specific consent, it would be prudent to check under which statutory power the information is being sought by the Government bodies and consider the relevant provisions carefully before proceeding with the disclosure.

Obligations to Protect Data – Why?



CODE OF
CONDUCT



Institute of Actuaries of India



United States

Code of Professional Conduct requires that an Actuary shall not disclose to another party any Confidential Information unless authorized to do so by the Principal or required to do so by Law.

An Actuary with knowledge of an apparent, unresolved, material violation of the Code by another Actuary should consider discussing the situation with the other Actuary and attempt to resolve the apparent violation.

If such discussion is not attempted or is not successful, the Actuary shall disclose such violation to the appropriate counseling and discipline body of the profession, except where the disclosure would be contrary to Law or would divulge Confidential Information.



Australia

Code of Professional Conduct requires that Actuaries to must take reasonable steps to ensure that the information used and the result of any Professional Services provided remain confidential to the extent expected by the Principal and that the Principal is made aware if there is a breach of confidentiality.

In circumstances where the Principal does not address and, if necessary, rectify any misuse within a reasonable time, and maintenance of confidentiality is or is likely to be Materially damaging to third parties, the Member:

- ✓ must obtain legal or other relevant professional advice, and
- ✓ take the appropriate action required. Also, in such circumstances the Member must consider whether, in the context of his or her legal obligations, there is a greater obligation to such third parties than the maintenance of confidentiality.

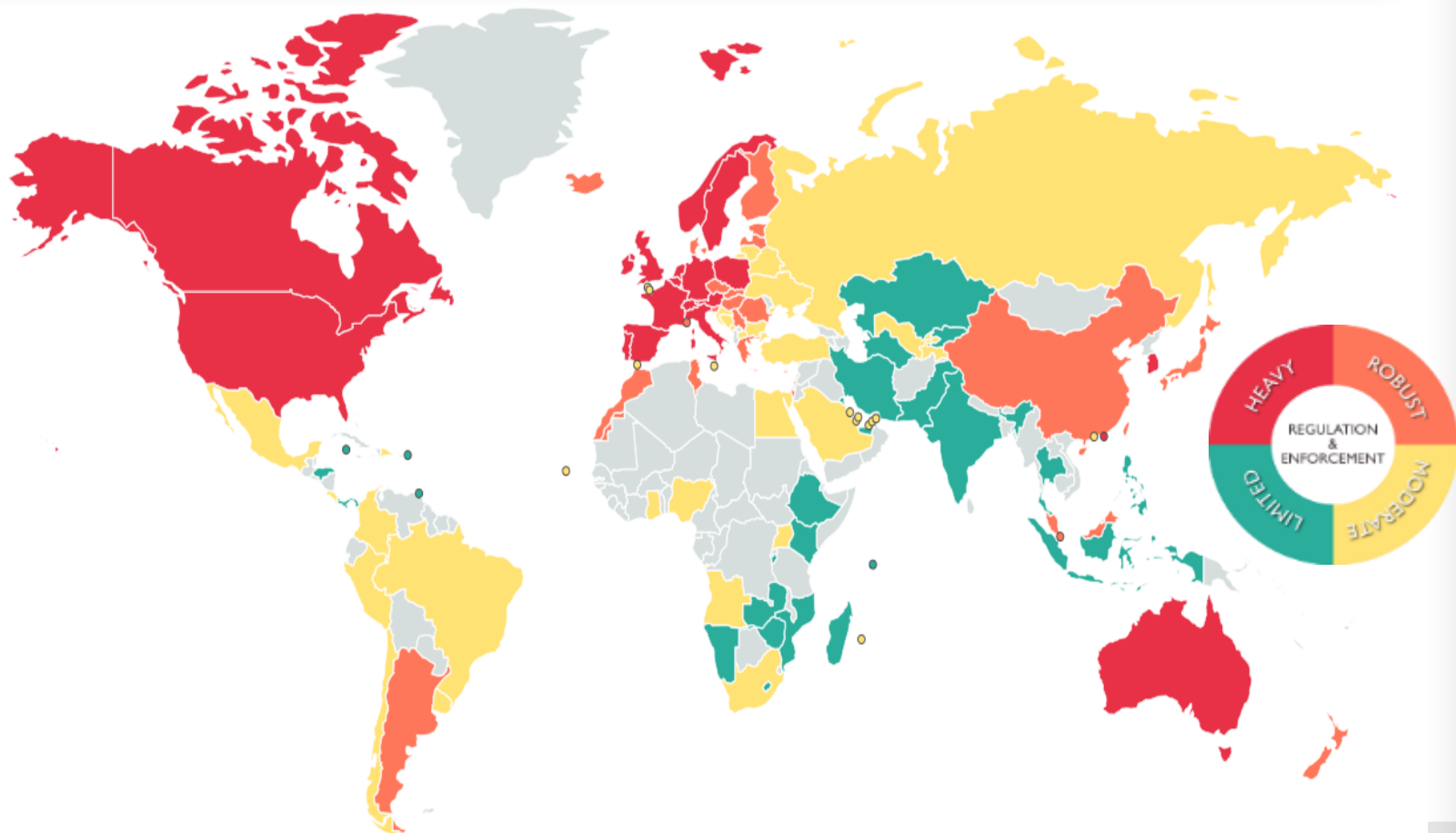
Obligations to Protect Data – Why?



LEGAL OBLIGATIONS



Laws, Regulations around the world requires Companies, employees and professionals to comply with legal provisions for the protection of Data.



Obligations to Protect Data – Why?



LEGAL
OBLIGATIONS



Global privacy laws are proliferating (<60 in 2009; >120 in 2019)

Latest in Asia

- Changes to the Privacy laws in: Japan, South Korea, Singapore
- New law in: Vietnam
- Proposed new Law in India

New Privacy Laws post GDPR

- Brazil LGPD (Lei Geral de Proteção de Dados)
- South Africa
- US: The California Consumer Privacy Act (CCPA) (and other States)

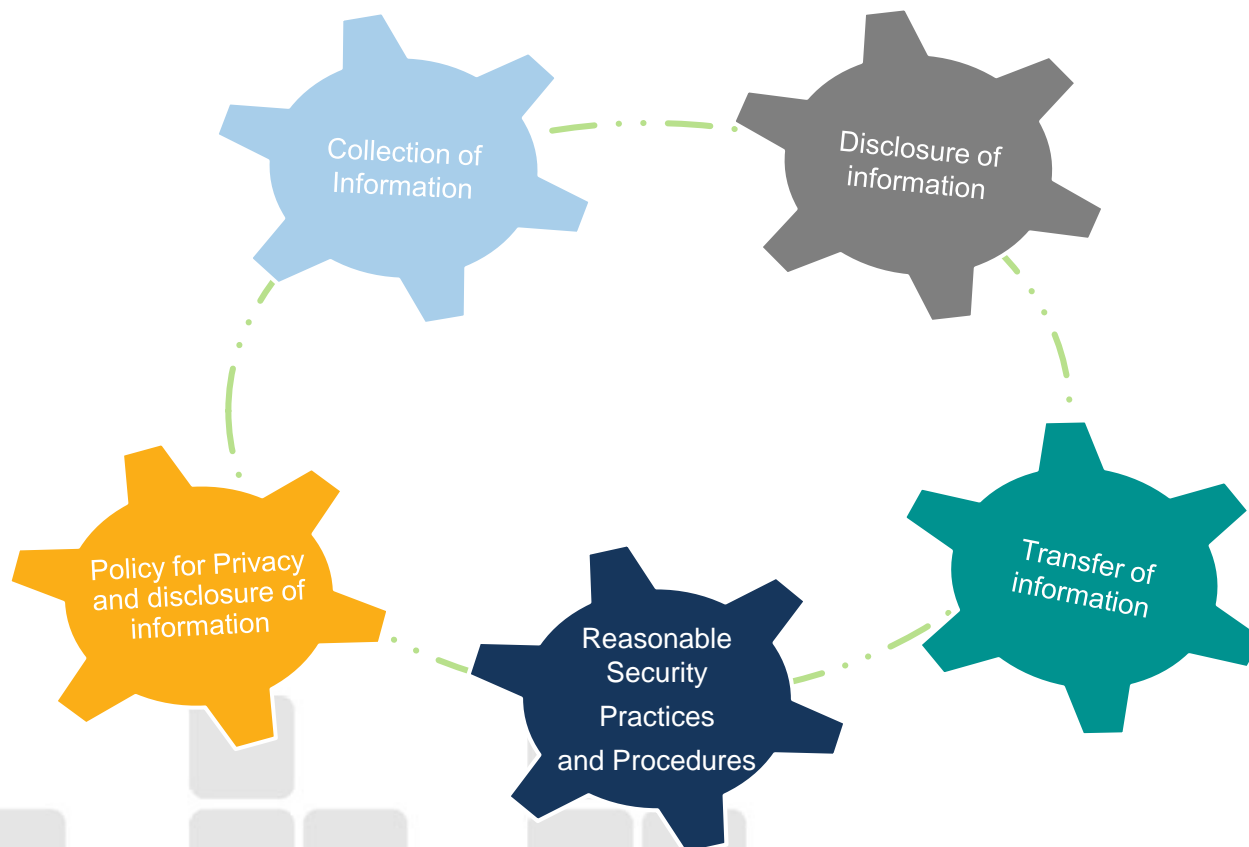
Obligations to Protect Data – Why?



LEGAL OBLIGATIONS



The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("IT Rules") provides legal requirements w.r.t.:



Obligations to Protect Data – Why?



LEGAL OBLIGATIONS



Data privacy Laws – India – IT Rules

The body corporate or any person who on behalf of body corporate

- ✓ collects
- ✓ receives
- ✓ possess
- ✓ stores
- ✓ deals or
- ✓ handle information of provider of information

shall provide a privacy policy for handling of or dealing in

- ✓ personal information including
- ✓ sensitive personal data or information

and ensure that the same are available for view by such providers of information who has provided such information under lawful contract.

The policy shall provide for:

- ✓ Clear and easily accessible statements of its practices and policies
- ✓ Type of personal or sensitive personal data or information collected
- ✓ Purpose of collection and usage of such information
- ✓ Disclosure of information including sensitive personal data or information
- ✓ Reasonable security practices and procedures



Policy for Privacy
and Disclosure of
Information

Obligations to Protect Data – Why?



Data privacy Laws – India – IT Rules

Body Corporate shall:

- ✓ obtain **consent** in writing from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.
- ✓ holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.
- ✓ keep the information secure.
- ✓ not collect sensitive personal data or information unless
 - the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
 - the collection of the sensitive personal data or information is considered necessary for that purpose
- ✓ take such steps (while collecting information directly from the person concerned) as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of
 - the fact that the information is being collected
 - the purpose for which the information is being collected
 - the intended recipients of the information and
 - the name and address of
 - the agency that is collecting the information and
 - the agency that will retain the information.

The information collected shall be used for the purpose for which it has been collected.



Collection of
Information

Obligations to Protect Data – Why?



Data privacy Laws – India – IT Rules

Critical elements:

- Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation

The third party receiving the sensitive personal data or information from body corporate or any person on its behalf shall not disclose it further.

- any sensitive personal data or information shall be disclosed to any third party by an order under the law for the time being in force
- The body corporate or any person on its behalf shall not publish the sensitive personal data or information



Disclosure of
Information

Obligations to Protect Data – Why?



Data privacy Laws – India – IT Rules

A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules.


The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

A body corporate or a person on its behalf to implement such security practices and standards and have a comprehensive documented information security programme and information security policies that are commensurate with the information assets being protected with the nature of business.

In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies



Transfer of
Information



Reasonable
security practices
and procedures

Obligations to Protect Data – Why?



GDPR

The EU General Data Protection Regulation (GDPR) has increased privacy rights for individuals and obligations for corporations while giving regulators greater enforcement powers. Here's what you need to know:

BROAD APPLICATION

The GDPR applies to:



- EU Companies (and UK companies, post-Brexit)
- Companies outside the EU when they collect or process personal data in or from the EU
- “*Data controllers*” as well as “*data processors*”



The EU definition of *personal data* is very broad and includes all data related to an identified or identifiable individual.

The GDPR additionally expands the scope of “*sensitive personal data.*”

INCREASED CORPORATE OBLIGATIONS

The GDPR imposes increased or new obligations on “controllers” and “processors” including:

- 72-hour breach notification to the regulators
- A need to engage in “*privacy by design*” when developing new products, systems and processes
- Appoint *Data Protection Officers*
- Conduct *Privacy Impact Assessments* for projects with higher privacy risks
- Ensure appropriate technical & security measures are in place; these may include steps like *encryption* and *pseudonymisation* of data (where identifiable information is replaced with artificial identifiers)

Obligations to Protect Data – Why?



GDPR

INCREASED INDIVIDUAL RIGHTS

Individuals will have:

- A right to a detailed notice of what data is being collected and how it is being used
- Where consent is required, it must be affirmative and informed and revocable
- A right to access and correct personal data as well as to object to certain uses of it
- A right to request a copy of his/her personal data in a portable format
- A right to ask that his/her data be deleted from records
- A right to object to profiling or any sort of “secondary uses of data” (e.g., analytics)

SIGNIFICANT CONSEQUENCES

\$

- Reputational harm for non-compliance
- Client expectations
- Fines of up to 4% of annual global revenue or €20 million, whichever is greater

Breaches

What can constitute breaches?



TRUST OF CLIENTS

- Not complying with the data protection clauses of contract.
- Data sharing with wrong recipient company
- Compromising on data protection tools agreed with Client.
- Integrity issues – Data leakage by Employees



CODE OF CONDUCT

- Non-compliance of Professional Code of Conducts
- Non-compliance Company specific code of conducts, policies



LEGAL OBLIGATIONS

- Non-compliance of Country specific Laws w.r.t., the protection of PI, CI and SPDI, inter-company and inter-country data transfer
- Non-compliance of Global Laws such as GDPR covering EU and non-EU countries

Consequences of breaches



Reputational damage to the company



Damage to individual careers, loss of Management time, damage to client relationships



Financial loss by losing clients, legal penalties, litigation cost, potential liabilities



Imprisonment for violation of laws



Vulnerability - Angry ex-employees, Benefits to Competitors, Negative Media Reporting

Data Incidents



Incidents:

- A bank lost data regarding 4,500,000 customers, including names, birth dates, Social Security numbers, and bank account information, when a third-party storage company lost a backup tape. The settlement is yet to be determined.
- A financial services corporation lost almost 50,000 names, addresses, birth dates, and, in some cases, Social Security numbers, when a disk was stolen from a vendor. The settlement is yet to be determined.
- A web browser employee sold almost 100,000,000 e-mail addresses to a spammer. The settlement was about \$2 million.
- A telecommunications company settled its privacy violation case for about \$200 million.
- A large retailer settled its privacy violation case for \$5 million

Case Law:

Various Claimants v W M Morrison Supermarkets (UK):

Employer liable for data breach by employee seeking to damage it

In January 2014, Andrew Skelton, who at the time was employed by Morrisons as a senior IT auditor, secretly copied the personal data (including names, dates of birth, addresses, bank account details and salaries) of 99,998 Morrisons' employees on to a USB stick. In March 2014, he posted the data on a file-sharing website and tipped off local newspapers about the data breach. Although he had tried to conceal his identity he was subsequently arrested and prosecuted for fraud by abuse of position, unauthorised access to computer material with intent to commit or facilitate further offences, and the unlawful obtaining of personal data. He was convicted and sentenced to eight years' imprisonment.

The Court also held Morrisons liable for the breach.

An employer can be held vicariously liable for a deliberate wrongful act carried out by an employee, even if that act takes place in their own home, provided that a sufficient connection can be established between the nature of his job and the wrongful conduct complained of, and even in circumstances where the employee is motivated by a desire to damage the employer.

Facebook:

Facebook Inc. agreed to pay a record \$5 billion to resolve a U.S. investigation into years of privacy violations, a settlement that increases the board of directors' responsibility for protecting users' data while changing little about the company's lucrative advertising business.

The commission opened an investigation into Facebook last year after revelations that data mining firm Cambridge Analytica had gathered details on as many as 87 million Facebook users without their permission.

Google:

Google has agreed to pay a \$13 million settlement that could resolve a class-action lawsuit over the company's collection of people's private information through its Street View project.

Street View is a feature that lets users interact with panoramic images of locations around the world that launched in 2007. The legal action began when several people whose data was collected sued Google after it admitted the cars photographing neighborhoods for Street View had also gathered emails, passwords and other private information from wifi networks in more than 30 countries.

The company initially called the data collection "a mistake." However, investigators found Google engineers built software and embedded it into Street View vehicles to intentionally intercept the data from 2007 to 2010, according to court documents.

New York based company's confidential data compromised in Mumbai

Confidential data from a New York company that had been entrusted to Mumbai-based BPO Epicenter Technologies Pvt Ltd was compromised recently.

The email accounts of the New York-based debt recovery company, used to communicate with clients, were illegally accessed from outside the BPO.

One of the email addresses was allegedly accessed by a rival BPO company. According to the FIR, five employees of the BPO were given four confidential email IDs and passwords of the New York firm so that they could communicate with clients on behalf of the company. Later officials at the BPO learnt that the email accounts had been accessed from other computers and their passwords had been changed.

Under the terms of an April 2018 agreement between Epicenter Technologies and the New York firm, confidential data could not be accessed or used from outside the BPO. But Epicenter gave one of its employees, who had access to the four email accounts, a laptop that contained a list of the NY firm's clients, their email IDs and other confidential information. This employee has since left the BPO but has not returned the laptop. Given the alleged role of a competing BPO, police are also investigating whether this is a case of corporate espionage.

A case has been registered against unknown persons under sections 43A (compensation for failure to protect data), 66C (identity theft), 66D (cheating by personation by using computer resource) and 72A (disclosure of information in breach of lawful contract) of the Information Technology Act.

Our Responsibilities



Every one has an active obligation to maintain the security, integrity and privacy of the information we use every day.

- Never disclose Internal, Confidential or Restricted Information with any unauthorized person
- Share Personal Information with third parties for the legitimate Business requirements, in line with the law and company policies, and take steps to protect it in transit
- Every one is responsible for using Company Information and Technology in a way that is professional and appropriate, as well as secure
- Process Personal Information only as necessary for legitimate business purposes and retain Personal Information only as long as needed to meet operational and legal requirements
- Must encrypt Confidential Information and Sensitive Personal Information before sending it outside your Company
- Must comply with applicable laws and regulations—and often apply further safeguards when business requires the transfer of data, including Personal Information, across geographic borders or to other organizations
- If you discover that a colleague's, client's or third party service provider's Personal Information has been compromised, report it immediately to the concerned person or the department in the Company
- Must not, during or after employment with the Company, disclose non-public or confidential Company information to anyone, except as required by law or as per the Company policies

Our Responsibilities



- Proper storage of personal data can mitigate the risk that it will be stolen or lost.
 - First, encryption, the conversion of data into cipher text that cannot be easily viewed by unauthorized people, is a common approach.
 - Second, given that network access is regulated and laptops all too frequently are stolen, it's generally more secure to store data on networks rather than on laptops.
 - Third, older or internally developed software should be checked for its security.
- Actuaries may utilize a subcontractor who needs access to PI from time to time. In such case, the actuary should ensure that there is a written privacy contract with the subcontractor and that the contractor has (and follows) a privacy policy.

E.g. - an actuary provided benefit-statement information to a vendor responsible for producing the benefit communications and a privacy violation occurs, a court might find the actuary at fault if a written privacy contract didn't exist.

- Use secured tools for transfer the PI with authorised person.
- Ensure to have system in place to destroy in accordance to the Company policy, laws, legal hold.
- If the client does provide unnecessary private information, the actuary should return it and delete all traces of it from the employer's storage structure

Personal Data Protection Bill, 2018 (PDP) – Key Terminologies



Personal Data - Data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.

Processing - Operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

Sensitive Personal Data - Passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual,

The DPA will be given the residuary power to notify further categories in accordance with the criteria set by law.

Data - Includes a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means

Data fiduciary - Any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data

Data principal - the natural person to whom the personal data belongs to (an individual, a Hindu undivided family, a company, firm, state, juridical person).

Data processor - any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary.

Personal Data Protection Bill, 2018 (PDP) – Critical provisions



- **Transfer Of Personal Data Outside India**
 - **Critical Personal Data** as categorized by DPA, can be stored only on Indian servers.
 - Personal data (except sensitive personal data) **may be transferred outside India** under certain conditions. These include: (i) where the **central government has prescribed that transfers** to a particular country are permissible, or (ii) where the **Authority approves the transfer** in a situation of necessity.

Exemptions – state security, prevention, investigation, or prosecution of any offence, or personal, domestic, or journalistic purposes.

- **Processing of Personal Data** and **Sensitive Personal Data** may be permitted without consent of the individual, in cases such as for any function of Parliament or state legislature or if required by the state for providing benefits to the individual, required under any law, to respond to a medical emergency, threat to public health or breakdown of public order, for reasonable purposes specified by the Authority, related to activities such as fraud detection, debt recovery, and whistle blowing.
- Data Fiduciaries are required to implement appropriate mechanisms for age verification and parental consent before **Processing Personal Data of Children** (persons below the age of 18 years) based on volume, proportion and possibility of harm to children arising out of processing of personal data.

Exception: Where a notified guardian data fiduciary exclusively provides counseling or child protection services to a child, then such guardian data fiduciary will not be required to obtain parental consent.

Personal Data Protection Bill, 2018 (PDP) – Critical provisions



- **Right to be forgotten** - The data principal may restrict or prevent continuing disclosure of personal data, in cases where the
 - Applicability is determined by Adjudicating officer.
 - Restriction of disclosure of personal data overrides the right to freedom of speech and expression and the right to information of any citizen.
- The data fiduciary shall **retain personal data** only as long as may be reasonably necessary to satisfy the purpose for which it is processed. However personal data may be retained for a longer period of time if such retention is explicitly mandated, or necessary to comply under a law. Periodic review to be done in order to determine whether it is necessary to retain the personal data in its possession and shall delete personal data where it is not necessary to be retained.
- **Penalties** – The proposed Bill provides for Civil and Criminal liabilities.

Any data principal who has suffered harm as a result of any violation of any provision, by a data fiduciary or a data processor, shall have the right to seek compensation from the data fiduciary or the data processor as the case may be.

However **a data processor shall be liable** only:

- ✓ where it has acted outside or contrary to the instructions of the data fiduciary or
- ✓ where the data processor is found to have acted in a negligent manner, or
- ✓ where the data processor has not incorporated adequate security safeguards as per the Bill
- ✓ or where it has violated any provisions of the Bill.

Personal Data Protection Bill, 2018 (PDP) – Data Protection Obligations



- ❖ Personal data must be fairly and lawfully processed for limited purposes.
- ❖ Information regarding data processing must be notified to Data Principle. Such notification must be easily comprehensible and in multiple languages where necessary.
- ❖ Personal data must be adequate, relevant and not misleading.
- ❖ Personal data must be accurate and up to date and Personal Information must not be kept longer than it is necessary.
- ❖ Personal data can be transferred to other countries only when authorized by the State.
- ❖ The data fiduciary shall only engage, appoint, use or involve a data processor to process personal data on its behalf through a valid contract.
- ❖ The data processor and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary unless they are required to do otherwise under law and shall treat any personal data that comes within their knowledge as confidential.

Competitive Advantage



Achieving effective and efficient compliance and having high standards of conducting business are **competitive advantages**

Adds value and improves organizational performance

Ensures compliance with regulatory and legal requirements

Exhibits professionalism allowing us to offer clients superior service standards

Maintains integrity and reputation of Company and its employees

Protects stakeholders: Clients, Shareholders, Employees, Regulators

We can distinguish ourselves from our competitors, strengthen our organization and be in a superior competitive position through both the quality of our work and our integrity and professionalism

THANK YOU !

Disclaimer:

This presentation is intended for educational purposes only and does not replace independent professional judgement. Statement or facts given in this presentation is based on the research of information/data available over various websites on the internet and other resources.