



**DSCI Sectoral Privacy Guide**

**Insurance**

Research Partner:



## **Disclaimer**

---

The content of the publication has been collected, analysed and compiled with due care based on the information and sources believed by DSCI to be reliable and available at the date of publication. However, DSCI disclaims all warranties as to the accuracy, completeness, or adequacy of such information. DSCI shall bear no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof. Readers of this publication are advised to seek their own professional guidance before taking any course of action or decision, for which they are solely responsible. It is highly advised to take note of the current Government and Sectoral regulations in place at the time of any practice implementation as they are subject to change from what has been represented now. The material in this publication is copyrighted but allowed for free distribution. You may not, however, modify, reuse or use the contents of the report for commercial purposes, including the text, graphics, presentations, etc. without DSCI's written consent.

**Copyright ©2022 | All rights reserved.**

# CONTENTS

<b>ABOUT THIS GUIDE.....</b>	<b>04</b>
<b>1. INTRODUCTION AND BACKGROUND .....</b>	<b>06</b>
The business of insurance .....	07
Data, Digitisation and “InsurTech” .....	08
The insurance sector in India.....	10
<b>2. KEY TERMS AND CONCEPTS IN THE GUIDE .....</b>	<b>13</b>
Insurance service provider and policyholder.....	14
Key data privacy terms .....	16
Tracing the journey of a policyholder .....	18
<b>3. THE CHALLENGE OF POLICYHOLDERS’ PRIVACY .....</b>	<b>22</b>
Ensuring compliance with existing regulations on data privacy .....	23
Preparing for emerging data privacy obligations.....	27
Managing disclosure of data to third parties.....	28
Addressing unique risks posed by new data sources and technologies .....	29
<b>4. INSURANCE CUSTOMER- CENTRIC PRIVACY PRINCIPLES .....</b>	<b>30</b>
Communicating effectively with policyholders.....	32
Obtaining informed consent from policyholders.....	36
Collecting accurate and proportionate personal data for providing insurance .....	41
Securing policyholders’ personal data.....	42
Using or disclosing personal data with the consent of the policyholder .....	46
for clear, specific, and lawful purposes	
Enabling policyholders to access and rectify their personal data.....	49
Using automated means of processing responsibly .....	52
Demonstrating compliance with best data protection practices.....	55
<b>5. SELF-ASSESSMENT CHECKLIST.....</b>	<b>59</b>
<b>6. REFERENCES.....</b>	<b>73</b>

# ABOUT THIS GUIDE

Digitisation has transformed how businesses are conducted across sectors. The increasing use of digital technologies and the internet has afforded new opportunities for efficiently and effectively reaching consumers and delivering services to them. These technologies have also made it easier than ever before to track, and profile consumer behaviour. It has become increasingly important to examine how the privacy of consumers and the protection of their personal data can be ensured during the consumer journey across sectors. This is essential to establish a relationship of digital trust between an organisation and its consumers.

This guide focuses on the insurance sector. It has been developed as part of a wider project of the Data Security Council of India (DSCI) to develop sectoral privacy guides for key sectors in India that are rich in consumer data (see Figure 1). It aims to help entities participating in the insurance sector move closer to embedding a privacy-preserving approach into their practices and operations. It is intended for privacy and security leaders employed by, and for privacy and security professionals working with such entities to implement privacy management programs. It will also be useful to personnel who regularly handle personal data about customers in their day-to-day activities.

The guide has two major components, a set of privacy principles and a self-assessment guide. The design of these principles and guide is centered around a consumer-centric perspective and arranged in accordance with the journey taken by consumers as they move through the insurance sector. This approach has been adopted to identify the touchpoints at which their data is collected and to underline the importance of understanding privacy from their perspective.

This guide has been created with the assistance of an advisory group of industry experts, namely Mr. Satyanandan Atyam, Chief Risk Officer of Tata AIF General Insurance Company Limited, and Ms. Neelakshi Shalla of Bharati AXA Life Insurance. The guide is curated after a series of stakeholder interactions with organisational experts and academic practitioners researching the scope of the Indian insurance sector. Exhaustive interviews were conducted with CISOs, directors, and professors hailing from IIT-Delhi and IIT-Bombay to SBI Life Insurance, LIC, ICICI Prudential, Max Life Insurance, IDBRT, SETU, etc.



## THE DSCI SECTORAL PRIVACY PROJECT

Since its inception in 2007, the Data Security Council of India (DSCI) has driven the development of industry standards, best practices, and initiatives on data privacy in India. DSCI has also consistently engaged with policymakers on efforts to develop laws and policies to strengthen the privacy and security culture in India. This includes the draft of Personal Data Protection Bill of 2019 (PDP Bill).

During our deliberations on the PDP Bill with stakeholders and experts, a consistent refrain that emerged was the need for deep dives on data privacy issues into specific sectors witnessing the collection of significant volumes of sensitive categories of personal data. This gave rise to DSCI Sectoral Privacy Project - an effort to develop sectoral guidance material for enterprises and organisations at all scales to understand and implement data privacy principles and controls as applicable to their sectoral context. Three sectors were identified as a starting point: health, insurance, and banking.



# 1 INTRODUCTION AND BACKGROUND



## THE BUSINESS OF INSURANCE

### Insurance is a means to hedge against risks.<sup>i</sup>

Companies offering insurance, or insurers, promise to protect consumers from potential losses arising from uncertain future events in return for insurance premiums from consumers. Insurers enter into insurance agreements (commonly known as insurance policies) with consumers (“policyholders”) to define the insured risk, quantify the premium, and stipulate the duration of cover, limit of the cover and other terms and conditions. Insurers arrive at the terms and conditions in the insurance policy by assessing risks and exposures of policyholders. Insurance policies are issued when insurers underwrite these risks and exposures.

### This guide also uses the term “policyholder” as an umbrella term.

We use this term to refer to any consumer that is considering, or being assessed for, an insurance product (known as “prospects”); any consumer that is covered from risk by an insurance policy (known as “insureds”), and any consumer that purchases and owns the actual insurance policy itself. In practice, the insured and the executant can be different persons. For instance, a parent may buy insurance for their child, an employer for an employee, and likewise.

### Different insurers offer different insurance products.

The insurance sector is generally divided into life insurance, where an insurer makes a payout

to a beneficiary on the death of the insured or a defined date during the lifecycle of the policy or at the maturity of the contract and general insurance, where an insurer compensates for expenses and/or losses occurring due to illnesses, accidents, damages to property, or other risks (such as fire, marine, travel, home, motor, or health insurance). A connected activity is a reinsurance, where insurers transfer or cede risk to other companies, called reinsurers, through reinsurance schemes. This enables insurers to underwrite more business, limit their losses (especially in the case of large potential risks), better manage their risk portfolio and exposure, and protect their financial standing.

### Several insurance intermediaries also participate in the sector.

Insurers, reinsurers, and policyholders interact and transact with each other through a range of intermediaries. There are a variety of service providers involved in different activities in the insurance value chain, such as marketing and solicitation, distribution, or servicing of claims.<sup>ii</sup>

### The insurance sector is strongly regulated.

Since the sector is seen as relevant to the public interest and economic growth,<sup>iii</sup> the activities of insurance, reinsurance and insurance intermediation are usually regulated. Several countries have in place regulatory and supervisory frameworks designed to protect policyholders and monitor insurers’ risk profiles.<sup>iv</sup>



## DATA, DIGITISATION AND “INSURTECH”

### Insurance is a historically data rich business.

Since insurers cannot directly quantify future uncertain risks or the length of time for which policyholders will continue to pay premiums, they must rely on proxy statistics and information about the risk profile of policyholders to carry out the risk profiling of the prospects and policyholders.<sup>v</sup> Insurance laws also impose a duty on policyholders to disclose all material information to insurers needed to estimate insured risks. This is to correct for the information asymmetry arising from policyholders being incentivised to present themselves as low risk.<sup>vi</sup> Insurers may also seek to collect the financial records and credit histories of consumers in the financial sector that are maintained by credit rating entities. Regulatory requirements may also require insurers to keep detailed records of policyholders, policies, and claims.<sup>vii</sup> At scale, insurers often end up collecting and handling significant amounts of information about policyholders, either directly or through intermediaries. Much of this may often be sensitive for them. For instance, to offer someone health or life insurance, insurers often need access to the medical and financial records of a prospect.

### Digital technologies are transforming the insurance business through InsurTech.

Like other parts of the financial sector, insurance and reinsurance are also witnessing the arrival and adoption of a variety of emerging technologies and innovative business models built around insurance products. Such innovations are being referred to as “InsurTech” innovations and are being developed by both incumbent regulated entities and by newer technology firms or start-ups.<sup>viii</sup> Several factors

have been driving InsurTech adoption, including the potential posed by recent technological developments, the changing expectations of customers and the pressure to improve back-office efficiency to gain competitive advantages<sup>ix</sup>. The COVID-19 pandemic has also played a key role, by forcing insurers to find digital alternatives to offline distribution channels.<sup>x</sup> Some major technologies in the global InsurTech movement are big data, machine learning, internet of things, cloud computing, and distributed ledger technologies.<sup>xi</sup>

### Regulators are seeking to keep up with InsurTech in innovative ways.

InsurTech business models may create friction with existing regulatory frameworks. For instance, some start-ups wishing to serve as insurance intermediaries may find it difficult to meet existing capital or other regulatory requirements needed to gain authorisations. Such requirements, though necessary to protect consumers, can be difficult for newer companies to acclimatise to, becoming a barrier to new market entry. To account for such challenges without compromising on regulatory oversight, regulators across the world have established platforms, called “regulatory sandboxes”, to experiment with their business models under relaxed regulatory conditions.<sup>xii</sup> This approach, although nascent, is potentially having a positive effect for encouraging innovation. A recent study found that, in the United Kingdom, entry into such regulatory sandboxes has a positive impact on the capacity of start-ups to raise capital by reducing regulatory costs.<sup>xiii</sup>



### **A significant development is the increasing collection and use of “alternative data”.**

The increasing use of digital technologies is rapidly increasing data trails of prospects/policyholders across market segments. This has made it possible to efficiently collect and analyse vast amount of data about prospects/policyholders for use in underwriting, distribution, customer segmentation, and other financial decision-making. It is now possible to collect data about policyholders’ payment behaviour with other businesses and utilities, their personal spending habits, or their mobile application usage, lifestyle, social media usage, or geolocation histories. Such data may be used to assess the ability and willingness of a policyholder to pay premiums.<sup>xiv</sup> Such policyholder data collected from non-traditional

sources is increasingly being referred to as “alternative data”.<sup>xv</sup> These have significant value from a financial inclusion perspective since they make it possible to assess the risk of unbanked policyholders or those without prior credit or financial histories.

### **Increasing data collection and reliance on digital technologies pose data privacy concerns.**

The increasing collection of information about policyholders is giving rise to concerns regarding the protection of their privacy and the security of their information.<sup>xvi</sup> Due to increased data sharing, there is a risk of a potential increase in the unauthorised access to and use or transfer of such information to a wide variety of regulated and unregulated entities.



## THE INSURANCE SECTOR IN INDIA

### The Indian insurance sector is characterised by an insurance gap.

The current market size of the insurance sector - estimated to be US ~\$280 billion - accounts for ~1.7% of the global insurance market.<sup>xxvii</sup> The market is characterised by low rates of insurance penetration and density. As of 2019-20, insurance penetration for life and general insurance stands at 3.2% and 1% respectively, while the density stands at US \$59 and US \$19 respectively.<sup>xxviii</sup> This indicates that much of the population is still uninsured. A 2018 report from Lloyd's considered this "insurance gap" in India to be the second largest in the world and estimated it to be US \$27 billion in terms of absolute costs.<sup>xxix</sup>

### Expanding access and adopting innovations will be needed to close the gap.

It has been suggested that the insurance sector will need to focus on providing access to simpler, competitive, and innovative insurance products, using technology solutions to simplify the processes of documentation, underwriting and claims settlement<sup>xxx</sup>, expanding the range of available insurance products,<sup>xxxi</sup> improving accessibility to insurance in rural and urban poor areas, and encouraging greater private sector participation.<sup>xxxi</sup> A recent report from the NITI Aayog notes the importance of focusing on digital channels for health insurance sales to bring down acquisition and operational costs and increased access.<sup>xxxi</sup>

### India has an established insurance regulatory system.

The sector is regulated by the Insurance Regulatory and Development Authority of India (IRDAI). The primary legislations are the pre-independence Insurance Act of 1938 (Insurance Act) and the post-liberalisation Insurance Regulatory and Development Authority Act of 1999 (IRDAI Act). These are complemented by

several subject-specific laws, such as those for marine insurance<sup>xxiv</sup> or insurance for emergency goods and undertakings,<sup>xxv</sup> schemes involving insurance and other financial products,<sup>xxvi</sup> or for the regulation of professionals serving as actuaries.<sup>xxvii</sup> Beyond insurance-specific laws, other laws, such as those on companies, contracts, foreign exchange, anti money laundering, IT Act, or information technologies, also apply to the insurance sector. For instance, insurance policies must, as per contracts, adhere to the Indian Contract Act of 1872. Their dematerialised forms must adhere to the Information Technology Act of 2000 (Infotech Act).

### The duties of the IRDA are to protect policyholders and regulate the sector.<sup>xxviii</sup>

It uses a mix of licensing, regulations, codes of conduct and guidelines to promote, regulate and ensure orderly growth of the insurance and reinsurance business in India. A recent intervention in this direction includes the adoption of regulations on microinsurance products that are intended to target specific limited risks that are often relatively low in value whilst having a limited policyholder impact. The IRDAI has been exploring various distribution channels to drive better insurance coverage in the vulnerable section of the society through common service centres, digital channels, and even fuel pumps and cooking gas agencies.<sup>xxix</sup>

### India is already a promising InsurTech market.

Recent market research indicates a presence of at least 66 InsurTech companies in India today, making India the second largest InsurTech market in the Asia Pacific (after China).<sup>xxx</sup> A recent market report also notes that funding in India's InsurTech market has risen from US \$11 million in 2016 to US \$287 million in 2020.<sup>xxxi</sup> In order to keep up

with these developments, the IRDAI has also established its own regulatory sandbox. In August 2019, it issued regulatory sandbox guidelines,<sup>xxxii</sup> inviting companies to submit applications to test upcoming innovations in a controlled environment. It has granted 67 approvals across three tranches. Some promising InsurTech use-cases in India include:



## WEARABLE DEVICES

These are used by consumers to track their health, fitness, and activity levels by collecting data points such as location, sleep cycles, heart rate and physical activity.<sup>xxxiii</sup> Indian insurers have already started to partner with wearable technology companies to offer discounted trackers to customers.<sup>xxxiv</sup> These wearable devices help insurers underwrite better by tracking and collecting multiple health metrics and dietary choices to understand a customer's lifestyle better and offer the right premium. Insurers have also started offering discounts and gift cards to policyholders for achieving stipulated exercise targets to promote healthier lifestyles.<sup>xxxv</sup>



## TELEMATICS

These are used in the context of motor insurance. Here, premiums for auto insurance are varied across customers based on their driving habits under a “pay as you drive” model. To calculate these premiums, ISPs have partners with automakers to install “black boxes” to track an individual's unique driving patterns by recording various metrics, such as time, location, hard braking, cornering, and acceleration. Researchers have also developed systems to help monitor emotional factors, like driver fatigue, distraction, and drowsiness,<sup>xxxvi</sup> that can then be processed to generate risk factors for drivers and help vigilant drivers enjoy lower premiums.<sup>xxxvii</sup>



## BIG DATA AND MACHINE LEARNING

This is a term used to describe the application of sophisticated data analytical tools to huge data sets gathered from a wide range of sources. These tools commonly utilise methods and programs categorised as “machine learning” or as “artificial intelligence” to analyse data and make decisions based on that data.<sup>xxxviii</sup> A key feature of such programs is that they “learn from the data in order to respond intelligently to new data and adapt their outputs accordingly”.<sup>xxxix</sup> Several use-cases in the Indian context that are gaining traction are predictive analytics and robo-advisory in underwriting, customer segmentation, distribution and claims settlement.<sup>xl</sup> For example, an Indian insurance company has launched a chatbot to underwrite micro-insurance products; another health insurance company has deployed AI's predictive algorithms to analyse previous years' claim activities and hospitalisation data to offer wellness incentives to customers towards keeping healthy.<sup>xli</sup> Many financial sector participants are also seeking to use machine learning technologies to engage with low-income users and to assess their creditworthiness.<sup>xlii</sup>

### **There is an increasing emphasis on data privacy in India.**

In August 2017, the Supreme Court of India, in the landmark Puttaswamy judgment<sup>xliii</sup>, laid down that the right to privacy is protected as a fundamental right under the Constitution of India. The ruling also recognized that this right is extended to the protection of personal information. As a result, policyholders in India are now guaranteed constitutional protection of their data privacy. The IRDAI is also now required to discharge a constitutional mandate to ensure the protection of policyholder information.

### **A comprehensive cross-sectoral data privacy law for India is expected soon.**

Following the Puttaswamy judgment, the Ministry of Electronics and Information Technology, in December 2019, also tabled a draft of a comprehensive data protection law for India called the Personal Data Protection Bill of 2019 (PDP Bill) and referred it to a Joint Parliamentary Committee on Data Protection (JPC). The JPC tabled its report accompanied by an amended version of the bill entitled Data Protection Bill, 2021. A key component of the Bill is the introduction of new rights for consumers in relation to their personal data.

It also establishes a new data protection authority that shall be empowered to regulate the use of personal data across sectors.<sup>xliv</sup>

### **The IRDAI has already started examining data-driven innovations from a privacy perspective.**

In 2017, the IRDAI constituted a working group to examine innovations in the insurance sector involving wearable and portable devices. Its report was released in July 2018. The report noted the need for regulations on protecting data privacy in terms of four dimensions: consent, usage, access, and disclosure.<sup>xlv</sup>

### **This guide aims to help the insurance sector prepare for the future of data privacy law.**

At the time of writing this report, the draft law has been reviewed by the JPC and its report is tabled before the parliament in December 2021. Once it becomes a law, the Data Protection Bill will overhaul existing data privacy law across sectors, including the insurance sector. This guide aims to help insurance sector participants protect the privacy of policyholders amidst this evolving regulatory environment and increasing pressure to adopt the use of digital technologies and alternative data to close the insurance gap in India.



# 2 KEY TERMS AND CONCEPTS IN THIS GUIDE



It is useful to set out some basic concepts and frameworks that are necessary to understand the challenges of policyholders' privacy. These are provided below.



## INSURANCE SERVICE PROVIDER AND POLICYHOLDER

This guide uses “Insurance Service Provider” (ISP) to refer to all entities that participate in the insurance sector and may handle the personal data of policyholders. This term captures insurers and reinsurers as well as a variety of

intermediaries and other service providers in the sector. Under the current legal and policy framework,<sup>xlvi</sup> the term “intermediary” includes:



**Individual and corporate agents** who represent insurers before the prospects and are appointed by insurers to solicit or procure business. They are usually tied to a single insurer with regards to a particular insurance product.<sup>xlvii</sup>

---



**Insurance and reinsurance brokers** represent, respectively, policyholders before insurers and insurers before reinsurers. Brokers can shop across multiple insurers for their clients.<sup>xlviii</sup>

---



**Insurance marketing firms** can be agents or brokers but are bound by fewer regulations.

---



**Insurance web aggregators**, recognised as intermediaries since 2017, are websites that offer comparisons of different insurance products. They earn from conversions on leads originating on their websites into purchases.

---



**Surveyors and loss assessors** estimate the quantum of loss occurring from a claim event.

---



**Common service centres** are e-governance service providers that offer insurance products in arrangements with insurers.

### Several other service providers also participate in the insurance sector.<sup>xlix</sup>

These include third-party administrators who assist in documentation collection or collect critical information to decide on claims on behalf of insurers during settlements; outsourcing service providers who take up several non-core functions for insurers otherwise performed by them; credit information companies who are regulated entities that collate loan and repayment behaviour of borrowers to create credit scores for use by financial institutions; account aggregators who are non-banking financial companies that provide individuals with consent and personal data management services; insurance repositories who store insurance policies in electronic form in a single location for the benefit of policyholders; and InsurTech companies who are using InsurTech innovations to offer services in different activities in the insurance value chain.

Beyond this, the Insurance Information Bureau is a non-profit set up by the IRDAI in 2009 to act as a sector-level data repository.<sup>i</sup>

### Some ISPs may be regulated under other regulatory frameworks.

It is to be noted that two of these entities – credit information companies and account aggregators – are regulated by the Reserve Bank of India (RBI) and not the IRDAI. Some entities may be simultaneously regulated by the IRDAI as well as by other financial sector regulators, such as banks who, when acting as corporate agents or brokers under bancassurance schemes, must comply with IRDAI regulations and RBI guidelines.<sup>ii</sup> Finally, some InsurTech companies may not be regulated by the IRDAI or by other financial sector regulators.



## KEY DATA PRIVACY TERMS



### Data

A term used to refer to collection of distinct pieces of information that are usually formatted and stored in a specific way, often for the purpose of reference or analysis. Data can include statistical information or facts, information about policyholders, as well as inferences derived from other data.



### Personal data

A term used to refer to data that contains a label, symbol or “identifier” that can be used to identify a specific policyholder or group of policyholders. All data collected while providing an insurance product to a policyholder is considered as personal data. Traditional sources of personal data in the insurance sector include proposal forms, customer health records, financial documents, claims settlement data and credit information. New sources of alternative data have also come up. The sources and types of such alternative data can include, for instance,

- Transaction data (such as from payment services, electronic commerce or other digitally tracked transactions)
- Telecommunications, rent and utility data
- Social media and networking data
- Audio and text data (e.g. collected through customer service calls or applications)
- App and clickstream data (collected as a customer uses an app or, for clickstreams, moves through a website)
- Internet of Things (IoT) which includes data from smart grids, smart devices and shipping and transport systems
- Crowdsourced data such as reviews from online communities and specialized social networks; weather and satellite data
- Survey and questionnaire data including psychometrics

<sup>lii</sup> Such data is still personal data when maintained or used in a state that enables the identification or tracing of a policyholder or group of policyholders. This term may also be called as personal information or policyholder information under different laws and regulations.



### Notice

A term used to refer to a set of public statements released by an entity that explains how it collects, uses, retains, and shares the personal data of any policyholder.





### **Data collection**

A term used to refer to various methods for procuring data of policyholders. In practice, this covers gathering, acquiring, or obtaining information from policyholders directly from them or other sources and collating these into a database. Examples of data collection activities include asking policyholders to fill up a proposal form; provide supporting documents, medical reports, collecting credit reports when conducting background verifications of their financial and health status; or collecting data about the medical treatment they may have received.



### **Consent**

A term used to refer to the affirmative action of giving consent, either orally or in writing, by an affirmative and unambiguous act.



### **Processing**

A broad term used to capture any activity performed by an insurer on personal data when that data is under their effective control. Examples of such activities include, with regards to data, collection, structuring, storage, alteration, adaptation, retrieval, indexing, disclosure, dissemination, erasure, or destruction.



### **Disclosure**

A term used to capture when an organization shares data with recipients outside its organization. ISPs need to frequently share policyholders' personal data with each other and to other organizations. For example, an insurance agent seeking to sell an insurance product to a policyholder will need to collect and share personal information – such as details filled in a proposal form – to the relevant insurer.



### **Anonymisation**

A term used to refer to different techniques that are used to remove 'identifiers' from personal data in an irreversible manner and to ensure that such data is no longer capable of being used to identify an individual, including in combination with other data.<sup>liii</sup>



### **Automated means**

A term used to refer to a system that may be made up of a combination of different hardware and software elements and may be used to make a decision with minimal or no human involvement.<sup>liv</sup> Examples of such decisions can include deciding to offer a micro-insurance product to a policyholder based on an analysis of their risk profile.

## TRACING THE JOURNEY OF THE POLICYHOLDER

The starting point to address data privacy risks and challenges is to determine how and when policyholders interact with ISPs and provide personal data to them. To do so, we adapted the methodology of customer journey mapping<sup>lv</sup> to map out the typical journey of a policyholder. In the interest of comprehensibility, we focus on the journey of one such policyholder in the life insurance sector. After reviewing the literature on mapping the insurance value chain<sup>lvi</sup> and incorporating insights from our discussions with stakeholders, we provide this map in Figure 4 to generalise the policyholders' journey across insurance products. Additional steps may be involved for different products. Here are the identified stages:

### Search:



The journey of a policyholder begins after they have identified the need for an insurance policy. This could be because of a life event. For instance, a policyholder may want to get a life insurance product after the birth of his/her child.

---



The policyholder will then try to gather information and seek advice on available options and providers. This may involve interacting with various insurers and intermediaries through online and offline channels. In recent years, insurers' websites and insurance aggregator websites have emerged as a key avenue for gathering information.

---



Insurers and a variety of intermediaries (such as agents and brokers) may also collect some personal data from the policyholder to assess their needs and determine their suitability for a particular insurance policy.

---



The policyholder may end up submitting some basic details containing personal data at this stage to a variety of ISPs to receive information and advice, such as their contact details, lifestyle habits, health records, income and other financial information.

### Selection:



The policyholder may receive a list of available options for the desired insurance policy, either from an agent, broker, or another intermediary, or through the interface of an online website. The policyholder may make their choice after comparing their features.

---



After selecting the option, the policyholder will most likely fill up a digital or physical proposal form.

## Onboarding:



The lifecycle of an insurance policy begins with the submission of the proposal form. A key stage during the onboarding of policyholders is the collection of consent for data processing, which traditionally is sought as part of the customer declaration or terms and conditions process of executing the insurance proposal form. This is a significant step since this will involve submitting consent to relevant third-party service providers for the collection of personal data as well as submitting significant amounts of personal data, including medical information, medical history, and financial data. The policyholder may also express their choice in relation to the use of electronic insurance policies.



The policyholder may then be expected to complete a Know-Your-Customer (KYC) process. The IRDAI has recently permitted the use of paperless KYC collection (or e-KYC) using Aadhaar-based authentication services offered by the Unique Identification Authority of India.<sup>lvii</sup>



After submitting the proposal form and completing the KYC process, the policyholder may be required to confirm submitted details through a verification process, such as verification call, or through a video-based identification process.<sup>lviii</sup> This is to determine if the policyholder is aware of the product he is opting for and other such submitted details.



ISPs may also conduct their own independent risk assessment exercises. They may collect the credit information of the policyholder or use other databases maintained by other financial service providers (such as on claims histories). They may also use third-party verification service providers, who may visit the policyholder to confirm details. In the case of some insurance products, such as life or health insurance, the onboarding process may also involve the policyholder getting a medical test done which involves data exchanges with a network of third-party administrators and medical centres.



After the onboarding process is complete, and no concerns are raised during the risk assessment and verification processes, the policyholder may receive the approval from the relevant underwriting entity.

## Purchase:



After receiving approval, the insurance contract is enforced, printed and dispatched/e-mailed to the policyholder. Sometimes a policyholder card is also sent. This is often used to signal that they have now entered in a formal agreement with the ISP and are covered as appropriate in that insurance policy.

---



ISPs may wish to use the services of an insurance repository to issue electronic insurance policies to policyholders. The IRDAI has clarified that all insurance policies in electronic form shall be treated as valid contracts.<sup>lix</sup>

---



The process of issuance of the insurance policy will likely involve the disclosure of the personal data of the policyholder to different intermediaries, such as insurance repositories, who will be mandatorily required to maintain records of issued policies.

## Use:



After owning the insurance policy, the policyholder will be required to pay regular premiums and insurers will continue to administer the purchased product during the term of the contract. New technologies have also made this easier. For instance, it is now possible for policyholders to pay insurance premiums using mobile applications and third-party payment wallets. This may involve the exchange of financial data between the policyholder, ISP, and any third-party service providers, including technology companies, involved in offering post-sales services to the ISPs.

---



During the term of the policy, if an insured risk occurs, the policyholder may wish to submit a claim to the ISP to receive a pay-out as per the policy. This may involve interacting with different ISPs involved in the claims settlement process, such as surveyors, loss assessors or third-party administrators. The entities involved may vary depending on the insurance product concerned.

---



ISPs will likely receive several types of personal data during the claims process. For instance, to determine if a claim is payable under a health insurance policy, an insurer may require the policyholder to submit detailed health and other appropriate information.

---



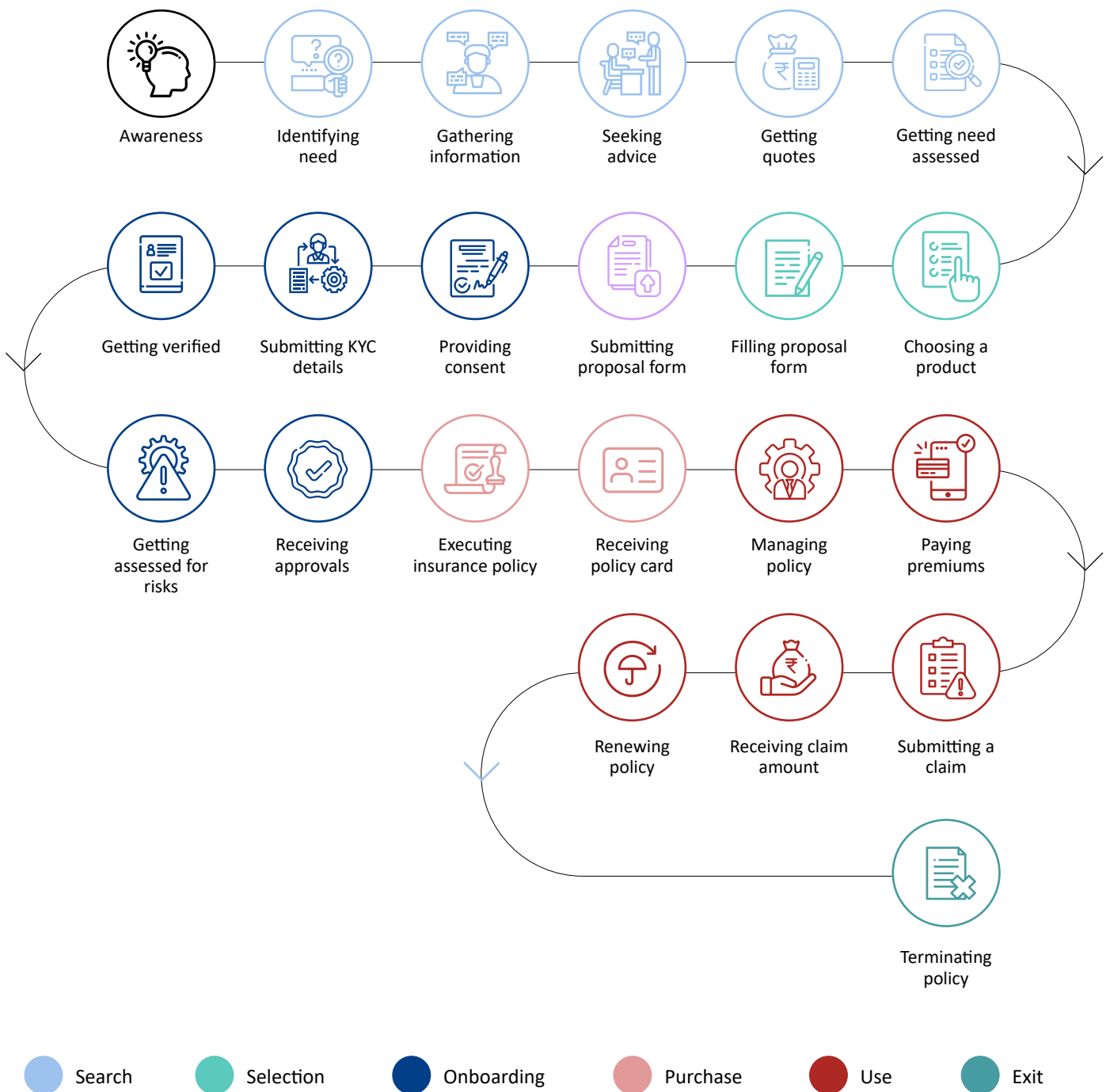
In the case of general insurance policies, the policyholder may choose to renew the policy. The renewal process may require the policyholder to complete a risk assessment process to determine if a fresh computation of the premium amount is required to reflect changes in the risk profile of the policyholder.

## Exit:



The policyholder may alternatively choose not to renew or surrender an insurance policy, triggering an exit from the lifecycle of that insurance product.

### Mapping the policyholders' journey in the insurance sector



# 3 THE CHALLENGE OF POLICYHOLDER PRIVACY



Due to recent technological, legal, and regulatory developments, ISPs face a wide range of risks and challenges from a data privacy perspective. We discuss these below.



## ENSURING COMPLIANCE WITH EXISTING REGULATIONS ON DATA PRIVACY

A patchwork of general laws and sectoral regulations impose several overlapping data privacy obligations on different categories of ISPs in India.<sup>lx</sup> This patchwork is broadly made up of the following:



### Cross-sectoral legislations:

This chiefly includes the Information Technology Act, which is the only law with provisions on data privacy that apply to private sector entities across all industries and contexts, including any ISP. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) set out general practices and requirements, including the publication of a privacy policy, the collection of consent for only lawful purposes connected to the activity, the appointment of personnel to handle complaints, or the adherence to recognised data security standards, such as the ISO/IEC 27001. Other relevant legislations include, for example, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Act) which regulates the use, masking and disclosure of Aadhaar information. Such legislations may contain penalties to address non-compliance with their data privacy requirements.<sup>lxi</sup>



### Financial sector regulations:

These may apply to different ISPs and their interactions with other participants in the financial sectors, such as account aggregators or credit information companies. They may impose conditions applicable to personal data. For instance, under the Credit Information Companies (Regulation) Act (CIRC Act), insures are entitled to receive credit information, but shall ensure that they take steps to implement a variety of privacy principles, when 'processing, recording, preserving and protecting the data relating to credit information' and security safeguards to ensure that the data relating to the credit information maintained by them is "accurate, complete, duly protected against any loss or unauthorised access or use or unauthorised disclosure thereof."<sup>lxii</sup>



### Sectoral laws and regulations:

Several different regulations and guidelines introduced by the IRDAI impose obligations on various ISPs and contexts that are intended to ensure policyholder privacy and confidentiality. A snapshot of the obligations under sectoral regulations on different ISPs is below.



Insurers<sup>lxiii</sup>

- Expected to maintain several records in electronic form in respect of all business transacted, including the name and details of all policyholders, their nominees and people making claims.
- Expected to have a data security policy that, inter alia, aims to secure the privacy and security of policyholder and claim data. Records should be organised in a manner that support policyholder service and compliance with applicable laws, regulations, circulars, guidelines, and other frameworks.
- Expected to hold records in data centers located and maintained in India only.
- May either directly or through any “distribution channel”, seek any information from a policyholder that the insurer considers necessary to “assess properly the risk covered under a proposal for insurance”. Policyholders are required to furnish all such information sought by the insurer.
- Expected to maintain, at all times, “total confidentiality of policyholder information”, unless required by law to disclose such information to a regulator or any statutory authority.
- Expected to check that any Outsourcing Service Providers (OSPs) used by them are purging the policyholders’ information after the contract terminates.
- Required to ensure that information and data parted to OSPs remain confidential; and policyholder data is retrieved with no further use of the same by the OSP once the outsourcing agreement is terminated.
- Expected to comply with detailed cybersecurity requirements, including the implementation of incident reporting mechanisms, security standards, audit requirements, governance requirements, data classification policies, etc. This includes introducing mechanisms for ensuring cybersecurity when sharing policyholders’ information with other regulated entities.
- In the context of health insurance, expected to comply with guidelines issued by IRDAI on “data related matters”. Expected to ensure the portability of health insurance policies across providers.





**Insurance brokers<sup>lxiv</sup>**

- Expected to treat all information supplied by the prospective clients as completely confidential to themselves and to the insurers to whom the business is being offered.
- Take appropriate steps to maintain the security of confidential documents in their possession.
- Expected to check that any outsourcing service providers used by them can enable the insurance broker to protect confidentiality and security of clients/ policyholders information.



**Insurance web aggregators<sup>lxv</sup>**

- Expected to treat all information supplied by the prospective clients as completely confidential to themselves and to the insurers to whom the business is being offered.
- Take appropriate steps to maintain the security of confidential documents in their possession.



**Insurance agents<sup>lxvi</sup>**

- Expected to treat all information supplied by the prospective clients as completely confidential to themselves and to the insurers to whom the business is being offered.
- Take appropriate steps to maintain the security of confidential documents in their possession.



**Common public service centers<sup>lxvii</sup>**

- Expected to treat all information supplied by the prospective clients as completely confidential to themselves and to the insurers to whom the business is being offered.
- Take appropriate steps to maintain the security of confidential documents in their possession.



**Surveyors and loss assessors<sup>lxviii</sup>**

- Expected to not disclose any policholder’s information to any third party, except, where consent has been obtained from the interested party, or where there is a legal right or duty enjoined upon him to disclose.
- Expected to ensure that they do not use any confidential information acquired or received by him to his personal advantage or for the advantage of a third party.



### Insurance repositories<sup>lxix</sup>

- Put in place measures to safeguard the privacy of the data maintained and adequate systems to prevent manipulation of records and transactions.
- Review the safeguards put in place continuously and submit half-yearly reports to the IRDAI regarding steps taken by it to maintain privacy of data.



### Third party administrators.<sup>lxx</sup>

- Expected to treat all information supplied by the prospective clients as completely confidential to themselves and to the insurers to whom the business is being offered.
- Take appropriate steps to maintain the security of confidential documents in their possession.



### Insurance Self-Network Platforms (ISNP)<sup>lxxi</sup>

- Expected to have adequate internal mechanisms to ensure “the privacy of data is maintained at all times” and to have in place data privacy measures and security safeguards that can prevent manipulation of records and transactions prior to commencing operations. Expected to comply with ISO standards.
- Expected to maintain confidentiality and prevent the misuse of personal information collected during an insurance transaction. Expected to ensure the privacy of persons using the ISNP is adequately protected.

### It can be challenging to frame the privacy expectations of policyholders vis-à-vis sectoral obligations.

As indicated above, under sectoral laws and regulations, the emphasis lies on ensuring ISPs adhere to record-keeping and data security requirements. However, such requirements, in relation to policyholders tend to be broadly worded, aimed at ensuring their “confidentiality”, without granular direction on how this may be operationalized in terms of meeting their expectations and needs from a privacy perspective. In the case of insurance intermediaries, obligations tend to be duplicated across regulations without any direction unique to their context or involvement in the insurance value chain.

### This makes it difficult to assure policyholders amidst rising data privacy awareness.

As discussed above, ISPs need to collect information from policyholders to determine the risk involved in offering them an insurance product and to fix the price of the product being offered to them. Policyholders are deterred from giving such information to ISPs that cannot assure them of their privacy. An increase in public debate and regulatory deliberations on data privacy has contributed to an increase in awareness around data privacy issues. Recent studies have shown that consumers across market segments may even prefer financial products offering privacy protections.<sup>lxxii</sup> Consumers’ data is also being shared widely across various entities in the consumer value chain. Some of these entities are small timer individuals or third parties which are operating in an unregulated sector and are only governed by a legal agreement with the ISP. The consumer is not aware of his data being shared across various entities and once known may be unwilling to share their data with third parties other than the principal provider of financial services.<sup>lxxiii</sup>

## PREPARING FOR EMERGING DATA PRIVACY OBLIGATIONS

### **A comprehensive data protection law is expected for India soon.**

As discussed in the previous sections, the DP Bill, once it becomes a law, shall likely induce a shift in the compliance obligations and mechanisms across the sector. It shall also impact the extent of the collection of policyholder data from different sources by ISPs. The DP Bill builds upon the existing regime to create a more nuanced and customer centric data protection regime.<sup>lxxiv</sup> The design and structure of the DP Bill is akin to those in other economies globally.<sup>lxxv</sup> At the time of writing, a key concern is the regulatory uncertainty. It is simply not clear what may or may not be permitted under the DP Bill. Industry representatives have questioned, for instance, whether the DP Bill, once it becomes a law, will regularise (or, alternatively, prohibit) the use of alternative data by credit information companies, ISPs, and other financial sector participants.<sup>lxxvi</sup>

### **ISPs will have to shift to a graded approach to protect personal data.**

The DP Bill will involve differentiated obligations for different types of personal data, where some may be considered as “sensitive”. A graded approach to personal data is not presently recognized. However, a recent example worth noting is from 2018, when the Delhi High Court passed an order stating that insurance products cannot provide for a broad exclusion of all genetic disorders. The order noted the need for a ‘proper framework to prevent against genetic discrimination as also to protect collection, preservation and confidentiality of genetic data’.<sup>lxxvii</sup> While this order was later stayed by the Supreme Court so that the IRDAI could be implemented,<sup>lxxviii</sup> the observations of the Delhi High Court are instructive from a data privacy perspective, as they point to the need for specific protections for certain categories of data that are especially sensitive from a privacy standpoint – such as genetic data.

### **Introducing processes for consent management for data collection.**

In our discussions with stakeholders, a key concern raised was that personal data was being collected without adequately informed or meaningful consent being collected from policyholders. The DP Bill will require entities to meet specific legally binding standards of consent and to disclose a wide variety of details about their data processing operations to consumers. This will also apply to the insurance sector. It is expected that new business models, such as account aggregators, that have recently been recognised in the financial sector, will play a key role in helping ISPs manage consent.

### **Complying with new transparency and accountability obligations.**

This is especially important considering the data-intensive nature of the industry. ISPs have historically processed different kinds of personal data like KYC records, health and financial data. Today, with the use of alternative data and new data processing technologies, ISPs are processing more and more granular personal data points.<sup>lxxix</sup> For instance, ISPs are processing near-real-time data from policyholders’ IoT devices or telematic devices to better understand policyholders’ lifestyle, and habits, to create a persona.<sup>lxxx</sup> ISPs may need to engage in a comprehensive process to adjust to these new regulatory requirements. ISPs can prepare for the new regime by designing strong customer-centric data protection practices that could facilitate compliance and simultaneously improve policyholders’ trust and uptake of insurance products and services.

## MANAGING DISCLOSURE OF DATA TO THIRD PARTIES

### The insurance value chain now has a complex mix of regulated and unregulated entities.

There can now be over 15 to 20 roles for service provision in various stages with multiple vendors filling these roles. Insurers can often have relationships and arrangements with numerous such vendors. At scale, it can be extremely difficult for ISPs to monitor the nature of their control over the data and the extent of their involvement in the processing of personal data in each case. The insurance value chain has also evolved to include technology service providers that can facilitate personal data flow and processing activities for ISPs.<sup>lxxxii</sup> ISPs must have robust data protection practices in this complex data ecosystem to safeguard policyholders' privacy. Adopting robust data protection practices, is therefore, becoming important for ISPs for complying with the emerging regulatory landscape.

### The use of digital technologies to enable third-party data access poses specific concerns.

The use of apps by intermediaries and other third-parties to collect personal data can result in the data being used for purposes other than what they were collected for. Mobile apps may also have ad-related components and expansive permissions to collect personal data without any linkage to a specified purpose. The use of Application Programming Interfaces (APIs) is also a concern. There are often no accepted standards for APIs; risks can arise from poorly designed and insecure APIs. In some cases, it is possible to misuse APIs to mirror and share personal information with third parties without adequate authorisation. There is a scope for a fraud being perpetuated from unauthorised data sharing and the leakage of policyholder data.<sup>lxxxiii</sup>

This is exacerbated by the lack of adequate oversight over such APIs and apps.

### Data sharing is a commercial necessity and regulatory mandate.

This challenge is exacerbated by present realities which require data sharing. As per insurers, the need to share policyholder data has become increasingly necessary due to the COVID-19 pandemic which has impacted the ability of ISPs to share data with each other. ISPs also need to meet regulatory requirements, such as to meet IRDAI guidelines requiring insurers to ensure policyholders can port their health insurance policies from one provider to another.<sup>lxxxiii</sup> ISPs are required to share data, including personal data of policyholders, with various regulatory and quasi-regulatory agencies. However, their precise data privacy obligations, applicable to regulators in relation to their data collection or disclosure practices is often unclear. In such a scenario, insurers face a key challenge to meet data sharing demands without compromising on policyholder's privacy.



## ADDRESSING UNIQUE RISKS POSED BY NEW DATA SOURCES AND TECHNOLOGIES

**Inaccuracy and bias in the insurance value chain are two key challenges posed by new data sources and technologies.**

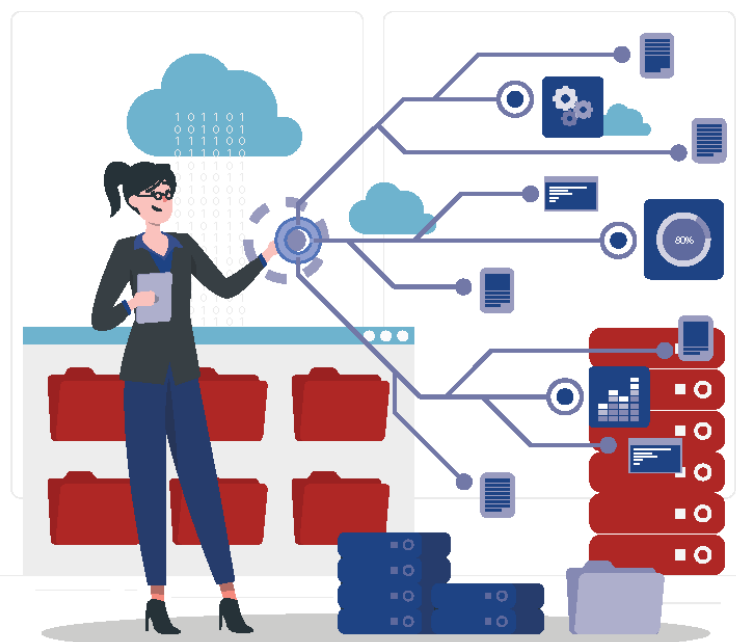
These can be used to drive insights related to historical transactional and health issues and behavioural patterns of customers. While these offer useful benefits, they also pose key challenges of inaccuracy and bias from the perspectives of data privacy and protection of policyholders. The use of automated means, for instance, can lead to incorrect assessments of policyholders or can perpetuate existing biases and risks posed to vulnerable communities at scale.<sup>lxxxiv</sup>

**Concerns with the increasing use of IoT devices offer insight into the challenge of inaccuracy.**

Consumer wearables are often transferred from the initial buyer to other persons who are the actual users. It is not clear if companies can discern this change of ownership. This creates scope for behaviours to be attributed to the wrong consumer.<sup>lxxxv</sup> In the context of auto insurance, advanced analytics platforms are required to ensure that usage-based telematics devices can differentiate between driving behaviour in different environments.<sup>lxxxvi</sup>

**Personalised premium calculation helps understand the challenges of bias.**

For instance, risk pooling models deployed by consumers could single out vulnerable consumers, putting them at a disadvantage and reducing opportunities for them to manage their risk.<sup>lxxxvii</sup> Regulators have noted that the increased use of data for personalized risk mapping in insurance could lead to consumer harms outside their control.<sup>lxxxviii</sup> There are also concerns of bias creeping into machine learning models reliant on data collected from IoT devices. For instance, there is increasing evidence to show that consumer wearables tracking various metrics, such as heart rates are more inaccurate when used by people with darker skin tones<sup>lxxxix</sup> or by people with tattoos, arm hair or thicker skin epidermis.<sup>lc</sup>



# 4 INSURANCE

---

# CUSTOMER-CENTRIC

---

# PRIVACY PRINCIPLES

---



Keeping these priorities for ISPs at the fore, we have identified a set of eight principles that provide them with actionable guidance to strengthen policyholders privacy and introduce data protection safeguards:



**Communicating effectively with policyholders:**

Notices that ISPs provide to policyholders must be simple, comprehensible and adequate. The notices should inform policyholders of how their personal data is collected, processed, stored, and shared, and the rights that policyholders have over their data.



**Obtaining informed consent from policyholders:**

ISPs must obtain consent from the policyholder before collecting personal data. The consent taken from policyholders must be informed, free, clear, specific and withdrawable.



**Collecting accurate and proportionate personal data for providing insurance services:**

ISPs must collect and process only that personal data that is accurate and necessary for fulfilling the purposes that policyholders have consented to.



**Securing policyholders' personal data:**

ISPs must adopt strong technical, managerial, operational, and physical security safeguards to protect the confidentiality and integrity of personal data throughout the data lifecycle.



**Using or disclosing personal data with the consent of the policyholder for clear, specific and lawful purposes:**

ISPs should use personal data or disclose personal data to third parties only with the policyholders' consent and for pursuing a clear, specific and lawful purpose.



**Enabling policyholders to access and rectify their personal data:**

ISPs should give policyholders access to their personal data and allow policyholders to rectify their personal data to ensure data accuracy. This is a current practice.



**Using automated means of processing responsibly:**

ISPs must complement the use of automated means of processing with adequate safeguards against risks, including, strengthening human oversight over automated means.



**Demonstrating compliance with best data protection practices:**

ISPs should be able to demonstrate their compliance with their stated data protection practices to the policyholders.

**PRINCIPLE 1****COMMUNICATING EFFECTIVELY WITH POLICYHOLDERS**

*Notices that ISPs provide to policyholders must be simple, comprehensible and adequate. The notices should inform policyholders of how their personal data is collected, processed, stored, and shared, and the rights that policyholders have over their data.*

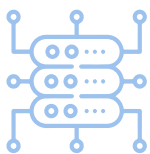
Providing easily accessible and comprehensible privacy notices about data processing activities is an important step in data protection.<sup>xc<sup>i</sup></sup> These notices serve two crucial objectives. First, the notices help ISPs gain the trust of policyholders, leading to greater uptake.<sup>xc<sup>ii</sup></sup> Second, the notices help policyholders better understand how their personal data will be processed and what it implies for them, improving their autonomy.<sup>xc<sup>iii</sup></sup>

This principle is also found in key regulations applicable to ISPs:<sup>xc<sup>iv</sup></sup>



**Cross-sectoral regulations** such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) which requires ISPs to provide a privacy notice to policyholders before collecting their personal data (Rule 4).

**Financial sector regulations** such as the Credit Information Companies Regulations, 2006 which requires ISPs to inform policyholders before collecting (or as soon as possible after collection) of their credit information (Rule 11(3)).



**Insurance sector regulations** like the IRDAI (Insurance Web Aggregators) Regulation, 2017 which requires specific insurance sector participants such as Web Aggregators to provide a notice (Sch. I Form R).



The key considerations for ISPs and measures they can take when providing notice to policyholders are set out below:



**i. Privacy notices must be designed in a user-centric manner so that policyholders can easily understand the provisions of the notice.**

- A privacy notice must not overwhelm or confuse policyholders by being too technical, specific or broad.<sup>xcv</sup>
- Information presented in the notice must be plain, clear, concise, easily comprehensible and adequately specific for policyholders to understand it properly.<sup>xcvi</sup>
- The notice must be made available in multiple languages when practicable.<sup>xcvii</sup>
- The notice must provide important information (like purpose for processing personal data or details of redress mechanisms) prominently.<sup>xcviii</sup>
- Provisions that request consent from policyholders must also be placed distinctly from the general provisions in the notice.<sup>xcix</sup>
- ISPs should present a privacy notice to policyholders just in time for data collection.<sup>c</sup>



**ii. Privacy notices must inform policyholders about the important aspects of personal data processing activities.**

- a. A privacy notice should clearly disclose:<sup>ci</sup>
- The types of personal data that will be collected, both, directly from the policyholder and indirectly from third parties;
  - The types of data that are mandatory and optional for a processing activity,
  - The purposes for which ISPs will process personal data, which must be clear, specific and lawful;
  - The duration for which ISPs will retain personal data;
  - The personnel and entities would be able to access the data;
  - The consequences of not providing personal data;
  - The third parties with whom the ISP may share data and instances of cross-border transfer of personal data, and
  - The security safeguards that the ISP adopted to safeguard personal data.
- b. The notice should also provide details about policyholders' rights over their data, grievance redressal mechanisms and ways to report misuse or breach of data.



**iii. Privacy notices must clearly inform policyholders about the use of automated means.**

The privacy notice must inform policyholders—<sup>cii</sup>

- That their personal data may be processed by automated means;
- That they may interact with automated systems, and
- About mechanisms through which they can contest or seek an explanation of decisions reached through automated means.





## CASE STUDY

### PRINCIPLE 1

# Communicating effectively with policyholders

Lakshmi wants to purchase a health insurance policy. She accesses the mobile application of an ISP where she is asked to create a user account. The process to create the account requires Lakshmi to share her identification documents, contact and financial details. The process also requires her to accept the terms and conditions of the mobile application.

However, the mobile application does not direct Lakshmi to the terms and conditions and the privacy policy governing the application. As a result, Lakshmi is not able to understand why the ISP wants to collect such personal information and how the ISP will use her information. Lakshmi is alarmed and decides not to set up the account since she is not clear on how her information will be used.

The ISP should make the terms and conditions and the privacy policy governing the mobile application easily available to Lakshmi. This information must be provided before asking Lakshmi to create a user account so that she can make an informed decision about creating an account. The ISP should also display this information prominently on their website for public reference.

The information itself should be conveyed through a specific and short notice that explains the terms and conditions in a plain and simple language that Lakshmi can understand. Lakshmi should also have the option to ask for customer support for a better understanding of the privacy policy and the ISP's practices. Doing so would allow Lakshmi to make an informed decision about giving ISP the consent to process her personal data.



**PRINCIPLE 2****OBTAINING INFORMED CONSENT FROM POLICYHOLDERS**

ISPs must obtain consent from the policyholder before collecting personal data. The consent taken from policyholders must be informed, free, clear, specific and withdrawable.

Consent is a crucial part of data protection which enables policyholders to exercise choice and control over how their personal data is used.<sup>ciii</sup> Basing processing activities on policyholders' consent can help ISPs reduce policyholders' apprehensions about risks and build trust.<sup>civ</sup>

This principle is also found in key regulations applicable to ISPs:<sup>cv\*</sup>

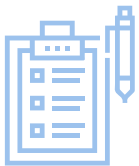


**Cross-sectoral regulations** such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) which requires ISPs to obtain consent for processing personal data and for sharing personal information with third parties (Rule 5 and rule 6).

**Financial sector regulations** such as the IRDAI (Insurance Web Aggregators) Regulation, 2017 require specific insurance sector participants like Web Aggregators which must take policyholders' consent in sharing personal data with insurers (Sch. I Form R).



The key considerations for ISPs and measures ISPs can take when obtaining consent from policyholders are set out below:



- i. By law, consent must be informed, free, clear, specific and withdrawable**
  - Policyholders must have all relevant information to give an informed consent.
  - Policyholders should give consent freely and voluntarily without being forced or misled.
  - Policyholders must give consent clearly and explicitly.
  - Policyholders must be able to give consent separately for the different purposes of processing personal data.
  - Policyholders should be able to withdraw their consent. Withdrawing consent must be as easy as giving consent.



## ii. Policyholders should not face barriers in giving or withdrawing consent.

- ISPs should allow policyholders to manage their consent preferences through entities such as consent managers.<sup>cvii</sup>
- Policyholders should be able to use the same channels for giving and withdrawing consent.
- To be accessible to less digitally savvy, less literate, or differently abled policyholders, the processes should:
  - a. Guide policyholders in understanding privacy notices and consent;
  - b. Provide alternate means of seeking and recording consent for differently abled policyholders, and
  - c. Help policyholders provide consent through visual and aural channels.



## iii. ISPs must design consent processes that strengthen policyholders' privacy.

- ISPs should disclose risks that could arise for policyholders from giving consent and the measures that ISPs have taken to mitigate those risks.<sup>cvii</sup>
- ISPs should disclose the use of automated systems for providing products and services to policyholders.<sup>cviii</sup>
- ISPs should not assume policyholders' consent by default. ISPs must take fresh consent from policyholders when they collect new personal data or begin new processing activities.<sup>cvix</sup>
- They must allow policyholders to opt-in and give explicit consent to processing activities.<sup>cx</sup>
- Policyholders must be able to refuse consent for optional processing activities without facing any detriment to the services they receive.<sup>cxii</sup>
- Policyholders should be able to withdraw their consent and opt-out of processing activities without detriment other than termination of services.<sup>cxii</sup>
- ISPs should maintain records of policyholders' consent preferences, consent withdrawals and correspondence when obtaining consent.<sup>cxiii</sup>



## CASE STUDY

### PRINCIPLE 2

# Obtaining informed consent from policyholders

Sarah is a visually impaired individual. With the assistance of her family, she had previously purchased a life insurance policy from an ISP. At the time of purchase, she had consented to the ISP to process her personal data according to the privacy notice that was given to her. However, Sarah was recently made aware of the changes to the privacy notice without her consent. Sarah did not want to consent to the changes and chose to withdraw her consent. On approaching her ISP, Sarah learns that the process for withdrawing consent is long-winded, and inaccessible to her as a visually impaired individual.

Sarah was not informed in advance about changes to the privacy notice. The ISP did not take her consent for processing her personal data under the new privacy notice. Furthermore, the ISP did not inform Sarah about the complex procedures for withdrawing consent when she purchased her insurance policy. These practices preclude Sarah from giving free, clear and informed consent, making it challenging for her to withdraw her consent.

In order to avoid this, ISPs must build consent artefacts that are accessible to policyholders facing a variety of barriers, including physical and mental disabilities. Further, the consent artefacts must allow policyholders to withdraw consent with the same ease as giving consent. ISPs must keep track of policyholders' consent preferences to understand the terms and conditions for which they have policyholders' consent, and those for which they must take consent afresh.



**PRINCIPLE 3****COLLECTING ACCURATE AND PROPORTIONATE PERSONAL DATA FOR PROVIDING INSURANCE**

ISPs must collect and process only the personal data, that is accurate and necessary for fulfilling the purpose that policyholders have consented to.

The personal data that ISPs process must satisfy two important criteria. First, ISPs must process only that personal data that is necessary for fulfilling the purposes that policyholders consented to. Processing unnecessary personal data could be intrusive and violate policyholders' privacy.<sup>cxiv</sup> Second, the personal data processed must be accurate. Processing inaccurate personal data can lead to inaccurate decisions, sub-optimal products and services, and poor financial outcomes for the policyholders.<sup>cxv</sup>

This principle is also found in key regulations applicable to ISPs:<sup>cxvi</sup>



**Cross-sectoral regulations** like the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) which requires ISPs to collect and process only necessary personal data (Rule 4 and rule 5).

**Financial sector regulations** like the Credit Information Companies (Regulation) Act, 2005 which requires ISPs to take measures to ensure credit information they process is accurate, complete and necessary for the purposes of processing (Chapter VI).



**Insurance sector regulations** like the IRDAI (Insurance Web Aggregators) Regulation, 2017 which require specific insurance sector participants like Web Aggregators to ensure data quality (Sch. I Form R(a)).

The key considerations for ISPs and measures they can take for ensuring data quality are set out below:



**i. The personal data collected and processed by ISPs must be proportionate and accurate.**

- Personal data processed by ISPs must be relevant and necessary for fulfilling the purpose of processing personal data.
- ISPs must delete personal data that is not necessary for processing.

- Personal data should be accurate, complete, representative, unbiased, up-to-date and not misleading.
- The collection of data to meet this quality should be consensual, lawful, fair and non-intrusive.
- ISPs should collect new personal data only if it is necessary for maintaining accuracy or fulfilling a purpose.<sup>cxvii</sup>
- ISPs should undertake data protection impact assessments to ensure they are only processing proportionate personal data.



## ii. ISPs must have mechanisms to verify the quality of personal data they process.

ISPs must:

- Frequently assess if the personal data being processed is inaccurate or out-of-date.<sup>cxviii</sup>
- Assess the quality and relevance of personal data for the purposes it is being processed.<sup>cxix</sup>
- Institute mechanisms to filter incomplete, inaccurate or unnecessary personal data during data collection.<sup>cxx</sup>
- Assess alterations in personal data from breach or cyberattack to rectify inaccuracies.<sup>cxxi</sup>
- Regularly review outputs from processing that are used as feedback or inputs for automated means of processing.<sup>cxxii</sup>
- Reviewing processing activities to identify and rectify causes of bad data quality.<sup>cxxiii</sup>
- Create protocols for assessing the quality of data collected from third parties.<sup>cxxiv</sup>
- Maintain records of the source from where personal data was collected.<sup>cxxv</sup>
- Maintain records of the measures taken to check accuracy of data.<sup>cxxvi</sup>
- Maintain records of inaccuracies and challenges to accuracy of personal data arising from policyholders' access rights.<sup>cxxvii</sup>





## CASE STUDY

### PRINCIPLE 3

# Collecting accurate and proportionate personal data for providing insurance

Khyaati has been a policyholder of a life insurance policy from an ISP for the past two years. She recently married Mathew and appended his surname to her last name. Khyaati wanted to change her name and update her personal information with her ISP. While updating her name, Khyaati realised that the ISP was processing some other personal information that was not only inaccurate but also not covered in the privacy notice.

So, she requested her ISP to delete unnecessary personal data and to rectify inaccurate data. The ISP denied Khyaati's requests because they did not have the means to identify unnecessary data and verify inaccurate data. The ISP continued to process personal data that was unnecessary and inaccurate for providing life insurance services. Khyaati felt that the ISP did not respect her privacy and interests, and terminated her relationship with the ISP.

ISPs must collect and process accurate personal data which must be necessary for fulfilling a purpose that policyholders' consent to. ISPs should establish mechanisms that can help examine accuracy and proportionality of personal data before and during the processing of personal data. ISPs can rely on different measures like performing Data Protection Impact Assessments (DPIAs), regularly reviewing the need to continue processing personal data, and allowing policyholders to access and rectify their personal data.



**PRINCIPLE 4****SECURING POLICYHOLDERS' PERSONAL DATA**

ISPs must adopt strong technical, managerial, operational, and physical security safeguards to protect the confidentiality and integrity of personal data throughout the data lifecycle.

Policyholders' privacy and the integrity of personal data are vulnerable to cyberattacks and data breaches. ISPs should take a variety of technical, managerial, operational and physical security measures that can protect the confidentiality and integrity of personal data throughout the data lifecycle. These measures must supplement other data protection practices like providing a privacy notice and obtaining consent. ISPs risk the reputation and integrity of processing activities in the absence of proper security safeguards.<sup>cxxviii</sup>

This principle is also found in key regulations applicable to ISPs:<sup>cxxix\*</sup>



**Cross-sectoral regulations** like the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) which requires ISPs to adopt security safeguards that can adequately protect the personal data that they process or share with third parties (Rules 8 and 9).

**Financial sector regulations** like the Credit Information Companies (Regulation) Act, 2005 which require ISPs to take measures to put proper security safeguards into place to protect credit information (Section 19, section 20, and section 22).



**Insurance sector regulations** like the IRDAI Guidelines on Information and Cybersecurity for Insurers, 2017 (cl.5 to cl.23) and the IRDAI Guidelines on Insurance E-commerce, 2017 (cl.10 to cl.15) which require ISPs to adopt a variety of data security safeguards.

The key considerations and measures that ISPs can take can take for ensuring robust data security safeguards are set out below:



**i. ISPs must identify the vulnerabilities and risks that must be addressed through security safeguards.**

ISPs must:

- Conduct information audits to understand vulnerabilities and risks to personal data.<sup>cxxx</sup>
- Conduct risk assessments and threat tests to understand risks to personal data.
- Conduct data protection impact assessments and threat analyses before using new technologies to process personal data.<sup>cxxxi</sup>
- Gauge the risk of re-identification for anonymised data through continuous review.<sup>cxxxii</sup>



**ii. ISPs must establish security safeguards that are proportionate to the risks identified.**

They must:

- Identify data protection guarantees in the privacy notice that must be operationalised through security safeguards.<sup>cxxxiii</sup>
- Adopt technological measures including encryption and use of passwords.<sup>cxxxiv</sup>
- Adopt organisational measures including defining data access, data authentication and authorisation protocols.<sup>cxxxv</sup>
- Adopt physical measures including security clearances to personal data servers.<sup>cxxxvi</sup>
- Deploy a data breach and incident management process that can—<sup>cxxxvii</sup>
  1. Help in addressing existing vulnerabilities and threats to personal data, and
  2. Help policyholders take steps to mitigate risks to personal data.
- Ensure personal data that is not relevant for processing is deleted or blocked when sharing with third parties;<sup>cxxxviii</sup>
- Ensure personal data is deleted carefully without giving access to unauthorised parties.<sup>cxxxix</sup>
- Implement anonymisation and de-identification techniques.<sup>cxl</sup>

- Periodically rectify automated means of processing based on audits and assessments.<sup>cxli</sup>
- Create controls to recover accidentally lost, altered or destroyed personal data.<sup>cxlii</sup>
- Regularly review security safeguards through audits, assessments and threat tests to identify and eliminate vulnerabilities.<sup>cxliii</sup>
- Implement and operationalise privacy-by-design principles<sup>i</sup> and security-by-design principles<sup>ii</sup> throughout the data lifecycle.



### **iii. ISPs must ensure security safeguards in sharing personal data with third parties.**

They must–

- Assess the risks that could arise from outsourcing personal data to third parties.<sup>cxliv</sup>
- Create controls to ensure third parties use personal data only to fulfil the purposes mentioned in their outsourcing agreement.<sup>cxlv</sup>
- Ensure that the third parties have adequate security safeguards to protect personal data.<sup>cxlvi</sup>
- Introduce breach notification requirements in outsourcing agreements with third parties.
- Incorporate measures to monitor personal data flows through Application Programming Interfaces (APIs) with third parties.
- Audit third parties using APIs for data malpractices.





## CASE STUDY

### PRINCIPLE 4

# Securing policyholders' personal data

“Insurall” is a leading health insurance provider in India that pioneers in using technology to support its services. Apart from collecting data from the policyholder, Insurall collects data indirectly from multiple sources. Insurall stores this data in a centralised database. It uses APIs to share information with authorised third parties for enhancing customer experience and for improving business opportunities.

Unfortunately, Insurall suffered a data breach which leaked highly sensitive policyholder information including payment transaction details, contact details and product purchase history. An independent investigation found that Insurall did not take measures to secure data that was shared to third parties. The APIs that Insurall used did not have strong security features that could protect personal data shared through them. Further, Insurall did not take proper measures to ensure that third parties with which it shared information had strong security safeguards. Hackers were able to exploit these vulnerabilities to access policyholders' data.

Insurall was negligent in implementing technical and procedural controls to ensure security of policyholders' data throughout the data lifecycle. Insurall made itself vulnerable due to improper oversight over its data practices. Insurall should have tested the APIs' security before using them and taken measures to address any vulnerabilities. Similarly, Insurall should have examined third parties' security practices for vulnerabilities that must be addressed through appropriate controls.



**PRINCIPLE 5****USING OR DISCLOSING PERSONAL DATA WITH THE CONSENT OF THE POLICYHOLDER FOR CLEAR, SPECIFIC, AND LAWFUL PURPOSES**

ISPs should use personal data or disclose personal data to third parties only with the policyholders' consent and for pursuing a clear, specific and lawful purpose.

ISPs may have primary purposes (like provision of insurance services), and secondary purposes (like cross-selling services or fulfilling legal and regulatory obligations) for using or disclosing personal data to third parties. Both, primary and secondary purposes, must be clear, specific and lawful. Further, in both cases, the ISPs must inform such use or disclosure to policyholders as part of their notice and take consent from policyholders before processing personal data. These measures can make processing activities more transparent and predictable for policyholders.<sup>cxlvii</sup>

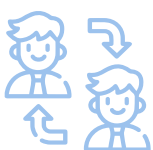
Further, policyholders should be able to request ISPs to disclose their personal data to other entities through data portability. Data portability allows policyholders to request ISPs to have their personal data transferred to any other entity in a machine-readable format.<sup>cxlviii</sup> This can help operationalise policyholders' autonomy over who their personal data is shared with.<sup>cxlvix</sup>

This principle is also found in key regulations applicable to ISPs:<sup>cl</sup>



**Cross-sectoral regulations** like the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) which requires ISPs to process personal data and disclose personal data for specific purposes and with policyholders' consent (Rules 5 and 6).

**Financial sector regulations** like the Credit Information Companies (Regulation) Act, 2005 which require ISPs to adopt principles determining what purposes credit information can be used for and when it can be disclosed (Section 20).



**Insurance sector regulations** like the IRDAI (Health Insurance) Regulations, 2016 provide for data portability, giving policyholders an option to transfer their personal data between ISPs (Schedule I of the Regulations).

The key considerations for ISPs and measures they can take to ensure appropriate data use and disclosure are set out below:



**i. ISPs should use or disclose personal data only for the clear, specific and lawful purposes that policyholders consented to.**

They must—<sup>cli</sup>

- Maintain a specific list of third parties to whom personal data may be disclosed.
- Disclose a list of purposes for which personal data may be disclosed to third parties.
- Stop disclosing personal data to third parties if policyholders withdraw consent.



**ii. ISPs must operationalise data portability for policyholders on their request.**

They must—<sup>clii</sup>

- Install mechanisms to receive and record data porting requests from policyholders.
- Adopt organisational policies and capacity to recognise and operationalise data porting requests.
- Verify the identity of the policyholder requesting for porting before transmitting data.
- Respond to porting requests in a timely manner.
- Receive and transmit personal data to third parties on policyholders' request.
- Transmit personal data on policyholders' request without placing financial, legal or technical obstacles.
- Transmit data on policyholders' request in a structured, commonly used and machine-readable format.
- Transmit data on policyholders' request in a secure method.



**iii. ISPs should maintain their assessments of policyholders distinctly from policyholders' personal data to aid data portability.**<sup>cliii</sup>



## CASE STUDY

### PRINCIPLE 5

# Using or disclosing personal data with the consent of the policyholder

Sameera wanted to purchase a health insurance policy that specifically covers diabetes. She approached an ISP who could meet her requirements. As part of the onboarding process, the ISP asked Sameera to share some personal information including her identification documents, contact details and medical history. Sameera read the terms and conditions about how the ISP uses personal information carefully and decided to share her information believing that it would be used only for providing insurance services.

A few days after sharing the information, Sameera began receiving messages from multiple fitness centres about special discounts for customers with diabetes. Alarmed by the messages, Sameera visited some of the fitness centres to find out how they got her contact details. She found that her ISP had shared her personal information with the fitness centres. Sameera read the ISP's privacy policy and her insurance agreement again to verify if she gave her consent to the ISP for sharing her personal information with the fitness centres. Neither of the document mentioned who the ISP can share Sameera's data with or for what purpose. The ISP disclosed Sameera's information to fitness centres without her consent. Sameera was compelled to give blanket consent and allow the ISP to share her data for secondary purposes which she did not prefer.

The ISP must stop disclosing Sameera's information to fitness centres and any other third party they may be disclosing information to. The ISP must clearly inform Sameera who they will share personal information with and for what specific purpose. The ISP should allow Sameera to consent separately for primary and secondary information sharing purposes. Sameera must be able to choose how her personal data is used and who it is shared with. Further, the ISP should not deny Sameera insurance services, the primary purpose for which her personal data was processed, because she denied consent for secondary purposes of processing personal data.





**PRINCIPLE 6****ENABLING POLICYHOLDERS TO ACCESS AND RECTIFY THEIR PERSONAL DATA**

ISPs should give policyholders access to their personal data and allow policyholders to rectify their personal data to ensure data accuracy.

Providing policyholders access to their personal data is an important part of upholding their autonomy<sup>cliv</sup> and maintaining data quality. Having access to information about processing activities can help policyholders stay informed and make decisions about how their personal data is used. In the same vein, policyholders will be able to identify inaccuracies in an ISPs' personal data records and rectify them. This would ensure ISPs process accurate data about policyholders.<sup>clv</sup>

This principle is also found in key regulations applicable to ISPs:<sup>cl</sup>



**Cross-sectoral regulations** like the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) which requires ISPs to enable access and rectification of personal data records by policyholders (Rule 5).

**Financial sector regulations** like the Credit Information Companies (Regulation) Act, 2005 which require ISPs to enable access and rectification of personal data records by policyholders (Section 20(a)(iii)).



**Insurance sector regulations** like the IRDAI (Health Insurance) Regulations, 2016 provide for data portability, giving policyholders an option to transfer their personal data between ISPs (Sch.I).

The key considerations for ISPs and measures they can take for enabling policyholders to access and rectify their personal data are set out below:



### **i. ISPs must establish processes for enabling access and rectification.**

They should—<sup>clvii</sup>

- Clearly communicate access and rectification process to policyholders.
- Facilitate policyholders' right to access personal data in a structured, machine-readable format.
- Enable access and rectification for personal data collected directly from the policyholder and indirectly from third parties.<sup>clviii</sup>
- Facilitate policyholders' ability to access and rectify their personal data when they choose without cost or delay.
- Allow policyholders to modify personal data through diverse channels including physical channels and digital portals.<sup>clvix</sup>
- Make changes to personal data records to match the modifications made by policyholders.<sup>clx</sup>



### **ii. ISPs should notify third parties about changes in personal data.**

They must—<sup>clxi</sup>

- Provide third parties with amended personal data records when necessary.<sup>clxii</sup>
- Take measures to ensure third parties rectify their personal data records.<sup>clxiii</sup>



### **iii. ISPs must provide policyholders information about important processing activities.**

They must—<sup>clxiv</sup>

- Give policyholders information about important processing activities, including processing through automated means.<sup>clxv</sup>
- Meaningfully communicate the implications, intended effects and rationale involved in automated means of processing.<sup>clxvi</sup>
- Demonstrate through prior assessments that automated tools provide legitimate outputs without discrimination.<sup>clxvii</sup>
- Provide policyholders with a standard list of third parties to whom personal data may be disclosed.<sup>clxviii</sup>



## CASE STUDY

### PRINCIPLE 6

# Enabling policyholders to access and rectify their personal data

After the occurrence of an accident, Alam visited an ISP-approved mechanic for repairing his car. The mechanic denied Alam's repair claim because the car's chassis number did not match the chassis number in the mechanic's records. Alam realised that the chassis number had been recorded incorrectly in the policy document. Alam contacted his ISP's customer care centre to ask about the procedure for rectifying the error.

The customer care executive told Alam that he must register himself on the ISP's web portal to make corrections. Alam asked for an alternative procedure because he could not use digital channels. The executive insisted that Alam use the web portal. Alam wrote a formal request to the ISP along with relevant documentation to rectify the date of purchase in the policy documents.

However, Alam did not receive a response from the ISP. As a result, Alam was unable to make a repair claim for his car.

ISPs must provide customers a variety of channels to access and rectify their personal data records. ISPs must also develop standard procedures to rectify personal data records and communicate rectifications to third parties promptly.



**PRINCIPLE 7****USING AUTOMATED MEANS OF PROCESSING RESPONSIBLY**

ISPs must complement the use of automated means of processing with adequate safeguards against risks, including, strengthening human oversight over automated means.

ISPs may use automated means for different purposes like assessing the risk profile of a policyholder. Outputs produced by automated means could pose unintended risks for ISPs and policyholders without adequate safeguards.<sup>clxix</sup> The risks for ISPs could include adverse selection and poor risk assessment of policyholders. The risks for policyholders could include unjust rejections, unsuitable products, and risks to privacy. Further, ISPs may be unable to understand or explain why automated means produce a certain output. ISPs should adopt and use automated means responsibly to avoid risk and protect policyholders' interests.

To comply with leading regulatory frameworks, ISPs can draw upon global best practices developed by practitioners and multilateral organisations. The key considerations for ISPs and measures ISPs can take for using automated means responsibly are set out below:

**i. ISPs must strengthen human oversight over automated means.**

They must—<sup>clxx</sup>

- Install measures to ensure transparency, auditability, accountability and explainability of decisions made by automated means.
- Explain the decision-making process of the automated means in clear, comprehensible and accessible terms.
- Record actions taken to identify, document and mitigate risks to policyholders' rights from automated means.
- Document the datasets and processes that automated means use to arrive at decisions.

**ii. ISPs must adopt safeguards against risks posed by automated means of processing.**

They must—<sup>clxi</sup>

- Preemptively identify risks to the safety and rights of policyholders from using automated means of processing by sandboxing or piloting.
- Ensure that the automated means are fit for the purpose of processing by clearly understanding the purpose for which they were developed, their capabilities and limitations.

- Test the robustness, reliability, accuracy, and security of automated means before putting them into use.
- Ensure that the data being processed is representative, unbiased and of high-quality.
- Debias personal data processed by automated means where necessary.
- Adopt best standards for gathering and labelling personal data that will be used for processing by automated means.
- Identify and address any bias in the decision-making process by automated means.
- Continually identify vulnerabilities in the automated means used for processing.
- Develop measures to mitigate the risks identified from automated means of processing.
- Upskill personnel who develop and administrate automated means of processing to ensure responsible processing.



### **iii. ISPs must give policyholders control over decisions made through automated means.**

They must–

- Notify policyholders through all service delivery channels that automated means may be used for making decisions about the policyholder.<sup>clxxii</sup>
- Allow policyholders to contest decisions made through automated means.<sup>clxxiii</sup>
- Create transparent processes for policyholders to submit complaints about decisions made through automated means.<sup>clxxiv</sup>
- Create a variety of channels for policyholders to contest or seek review of decisions made through automated means.<sup>clxxv</sup>
- Create clear processes for policyholders to seek redress when their rights are harmed by processing by automated means.<sup>clxxvi</sup>
- Provide data management tools that can help policyholders review, edit, and update personal data that is processed through automated means.<sup>clxxvii</sup>
- Make policyholders aware of their rights in relation to how their personal data is processed through automated means.<sup>clxxviii</sup>



## CASE STUDY

### PRINCIPLE 7

# Using automated means of processing responsibly

Anuj and Harshitha contracted dengue and were admitted into the same hospital and underwent the same treatment. Both their treatment cost the same and they filed claims with the same ISP under the same insurance scheme. However, the insurance company approved only a fraction of Harshitha's claim while Anuj's claim was approved in its entirety.

On raising the issue with the ISP, the ISP explained that claim settling is automated and they avail of the services of a vendor that provides that service. The ISP is unable to explain why Harshitha's claim was rejected even when Anuj's claim for the same amount and same medical condition was accepted in its entirety.

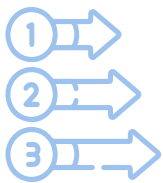
ISPs using automated means of processing must install strong controls, oversight mechanisms and customer safeguards. ISPs must be able to trace the decision-making process of an automated system and explain the decision in simple terms to customers. ISPs must also preemptively identify risks from using automated means, like discrimination between policyholders, and take adequate measures to mitigate those risks.



**PRINCIPLE 8****DEMONSTRATING COMPLIANCE WITH BEST DATA PROTECTION PRACTICES**

ISPs should be able to demonstrate their compliance with their stated data protection practices to the policyholders.<sup>clxxix</sup> They could adopt a variety of transparency and accountability measures to do so. Transparency and accountability play a crucial role in developing a relationship of trust with policyholders. Through transparency and accountability, ISPs can demonstrate and reassure policyholders that their personal data is being used safely and responsibly in a way that safeguards privacy.

The principle has been embedded into the existing data protection regime in India across different regulations. These regulations mostly aim to facilitate and ensure regulatory compliance. However, ISPs could leverage the same obligations to build trust with policyholders. Some key regulations are set out below.<sup>clxxx</sup>



**Cross-sectoral regulations** like the Information Technology Act, 2005 which requires providers intermediating information flows to maintain records of activities specified by the Central Government (s.67C). The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 also require ISPs to be able to demonstrate that they follow the best practices for data protection (Rule 8).



**Insurance sector regulations** like the IRDAI (Maintenance of Insurance Records) Regulations, 2015, the Guidelines on Insurance E-Commerce, 2017 and the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017 require ISPs to maintain records for a variety of processing activities, including outsourced processing activities. Some other regulations like the Guidelines on Insurance E-Commerce, 2017, the IRDAI (Insurance Web Aggregators) Regulations, 2017 and the IRDAI Guidelines on Information and Cybersecurity for Insurers, 2017 require ISPs to establish:

- Strong security safeguards;
- Protocols for independent audits of personal data processing activities;
- Risk assessment frameworks for outsourcing personal data processing activities, and
- Strong organisational measures to ensure confidentiality of personal data.

The key considerations for ISPs and measures they can take for ensuring accountability in processing activities are set out below:



**i. ISPs should create organisational capacity for personal data protection.**

They should:<sup>clxxxix</sup>

- Train their staff and personnel to answer inquiries about the ISP’s privacy policies, consent processes, security safeguards and redressal processes.
- Inform third party service providers about past vulnerabilities and attacks.



**ii. ISPs should demonstrate their compliance with data protection laws and best practices.**

They should:<sup>clxxxix</sup>

- Appoint personnel who would monitor the ISPs’ compliance with data protection law and ensure best practices in data protection.
- Publish the names of personnel responsible for ensuring the ISP follows robust data protection practices.
- Conduct audits to assess effectiveness of privacy notices, security safeguards and key data protection practices.
- Maintain records of different aspects of processing activities including–
  - a. The source from where personal data was collected;<sup>clxxxiii</sup>
  - b. The measures taken to check accuracy of data;[ Ibid. ]
  - c. The processing activities that were undertaken with the personal data;
  - d. The disclosure of personal data to third parties;
  - e. The security safeguards installed; and<sup>clxxxiv</sup>
  - f. The data protection impact assessments conducted prior to processing personal data.
- Develop, document and implement data policies defining –
  - a. The protocols for implementing a privacy by design policy
  - b. The protocols for collection, access and use;
  - c. The protocols for retaining and deleting personal data;
  - d. The means to ensure data quality;
  - e. The security safeguards and risk assessment frameworks;
  - f. The protocols for implementing a security by design policy;
  - g. The protocols for personal data breach and incident management, and
  - h. The protocols for imparting privacy training to personnel.





### iii. ISPs should have robust grievance redressal channels for policyholders.

They must—<sup>clxxxvi</sup>

- Have effective, efficient, speedy and time-bound grievance redressal mechanisms that can help policyholders resolve data-related grievances.
- Publish details of the Grievance Redressal Officer (GRO) and the data protection officer clearly in the privacy notice.
- The redressal mechanisms should have simple procedures that do not burden policyholders.
- Policyholders should be able to seek redressal through different digital and physical channels.
- ISPs should leverage technology to create better feedback loops with policyholders.





## CASE STUDY

### PRINCIPLE 8

# Demonstrating compliance with best data protection practices

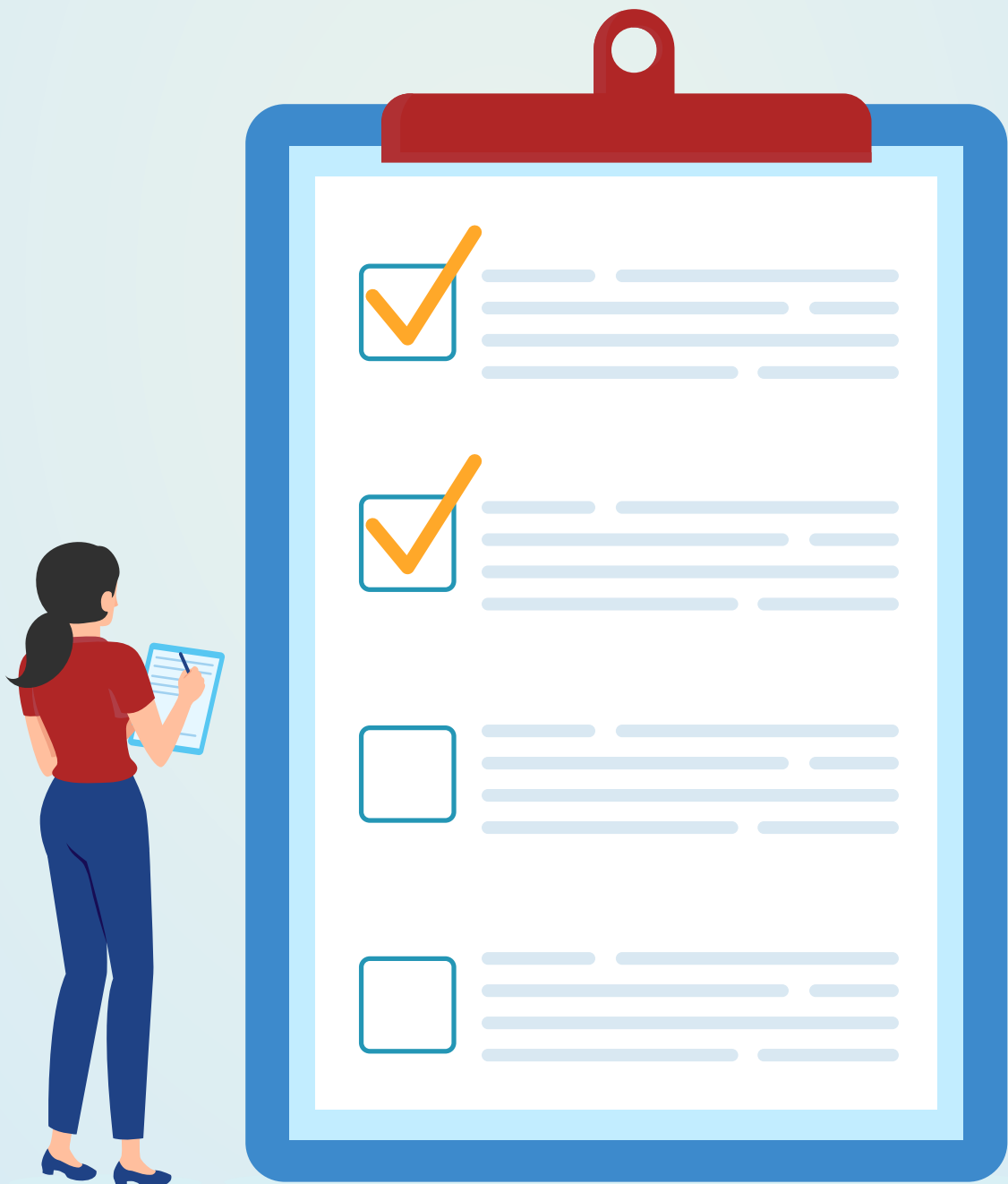
Michael has a reason to believe that someone is trying to use his personal information and contact details to breach his insurance account information. Michael contacts his ISP to notify them about the suspicious activity and safeguard his account. Michael soon realises that his account had been hacked and his personal information had been altered.

Michael tries to register a formal grievance with the ISP for not preventing the incident. The ISP denies any role in the incident claiming to have robust practices and rejects Michael's complaint. Shortly after, reports surface about a major data breach from the ISP's technology partner's servers. The technology partner did not take sufficient measures to safeguard customers' data from breaches and cyberattacks. When Michael approaches the Ombudsman, it becomes apparent that the ISP did not take adequate measures to ensure its partners maintain adequate data protection and security safeguards.

ISPs must be able to demonstrate that they and their partners comply with best data protection practices. For this, they must–

- Establish procedures to ensure third parties have robust data protection and data security practices.
- Establish procedures including developing data protection policies, keeping records of data processing activities, auditing data protection practices etc.
- Create capacity within the organisation and appoint personnel to engage with data protection-related queries and concerns from customers.
- Create robust grievance redressal channels that can effectively and speedily provide redress to customers, and also help ISPs identify vulnerabilities in their systems and practices.

# 5 SELF-ASSESSMENT CHECKLIST






**PRINCIPLE 1:**

**COMMUNICATING EFFECTIVELY  
WITH POLICYHOLDERS**

- 
- Does the ISP provide a privacy notice to the policyholder?
  - Is the privacy notice drafted in the preferred language of the policyholder?
  - Is the privacy notice written concisely?
  - Is there an aural privacy notice available for those unable to read?
  - Is the privacy notice written in simple, plain and easily understandable language?
  - Is the privacy notice presented just before data collection?
  - Does the privacy notice prominently disclose the purposes for processing personal data?
  - Is the purpose communicated in the privacy notice, clear, specific and lawful?
  - Are the provisions that request consent from policyholders placed distinctly from the other provisions in the notice?
  - Does the privacy notice disclose the types of personal data that will be collected directly from the policyholder?
  - Does the privacy notice disclose the types of personal data that will be collected indirectly from third parties?
  - Does the privacy notice disclose the types of data that are mandatory for a processing activity?
  - Does the privacy notice distinctly disclose the types of data that are optional for a processing activity?


- 
- Does the privacy notice disclose the implications for policyholders if they do not provide personal data?
  - Does the privacy notice disclose the procedure policyholders can follow to withdraw consent?
  - Does the privacy notice disclose the duration for which personal data will be retained?
  - Does the privacy notice disclose the details of all the personnel and third parties who will be able to access the data?
  - Does the privacy notice disclose the identities of third parties with whom data may be shared?
  - Does the privacy notice disclose the purposes for which personal data may be transferred across borders?
  - Does the privacy notice disclose the instances in which personal data may be transferred to another jurisdiction with inadequate data protection safeguards?
  - Does the privacy notice disclose the security safeguards that have been adopted to safeguard personal data?
  - Does the privacy notice disclose policyholders' rights over their personal data?
  - Does the privacy notice disclose the use of automated means in processing data?
  - Does the privacy notice prominently provide details about grievance redressal mechanisms for reporting misuse or breach of data?
  - Have the details of the grievance redress officer and the data protection officer been published clearly in the privacy notice?
  - Does the privacy notice inform how policyholders can contest or seek explanation for decisions made through automated means?



**PRINCIPLE 2:**

**OBTAINING INFORMED  
CONSENT FROM POLICYHOLDERS**

- 
- Have policyholders been given all the information about how their personal data will be processed?
  - Have policyholders been given information about primary and secondary purposes for processing personal data?
  - Are policyholders informed of the potential risks of giving consent?
  - Are policyholders informed of measures that have been taken to mitigate risks to personal data?
  - Are policyholders informed of the use of automated systems for providing products and services?
  - Have the policyholders been briefed about the rationale, implications and intended effects of processing personal data through automated means?
  - Do any of the terms and conditions in the notice make it hard for policyholders to give consent freely?
  - Can policyholders seek guidance in understanding privacy notices and the implications of giving consent?
  - Is consent taken expressly from policyholders?
  - Are policyholders allowed to give consent separately for the different purposes of processing personal data?

- 
- Are policyholders allowed to withdraw their consent as easily as they were able to give consent?
  - Are policyholders allowed to manage their consent preferences through entities like consent managers?
  - Do policyholders have a common channel for giving and withdrawing their consent?
  - Are policyholders allowed to provide consent through visual and aural channels?
  - Have processes been designed to provide notice and take consent from differently-abled policyholders?
  - Is fresh consent taken from policyholders when new personal data is collected, or new processing activities are started?
  - Are policyholders able to withdraw their consent for mandatory processing activities without detriment other than termination of services?
  - Can policyholders refuse consent for optional processing activities without facing detriment to the services they receive?
  - Are policyholders charged fee for withdrawing consent?
  - Are records maintained of policyholders' consent preferences, consent withdrawals and correspondence at the time of obtaining consent?



### PRINCIPLE 3:

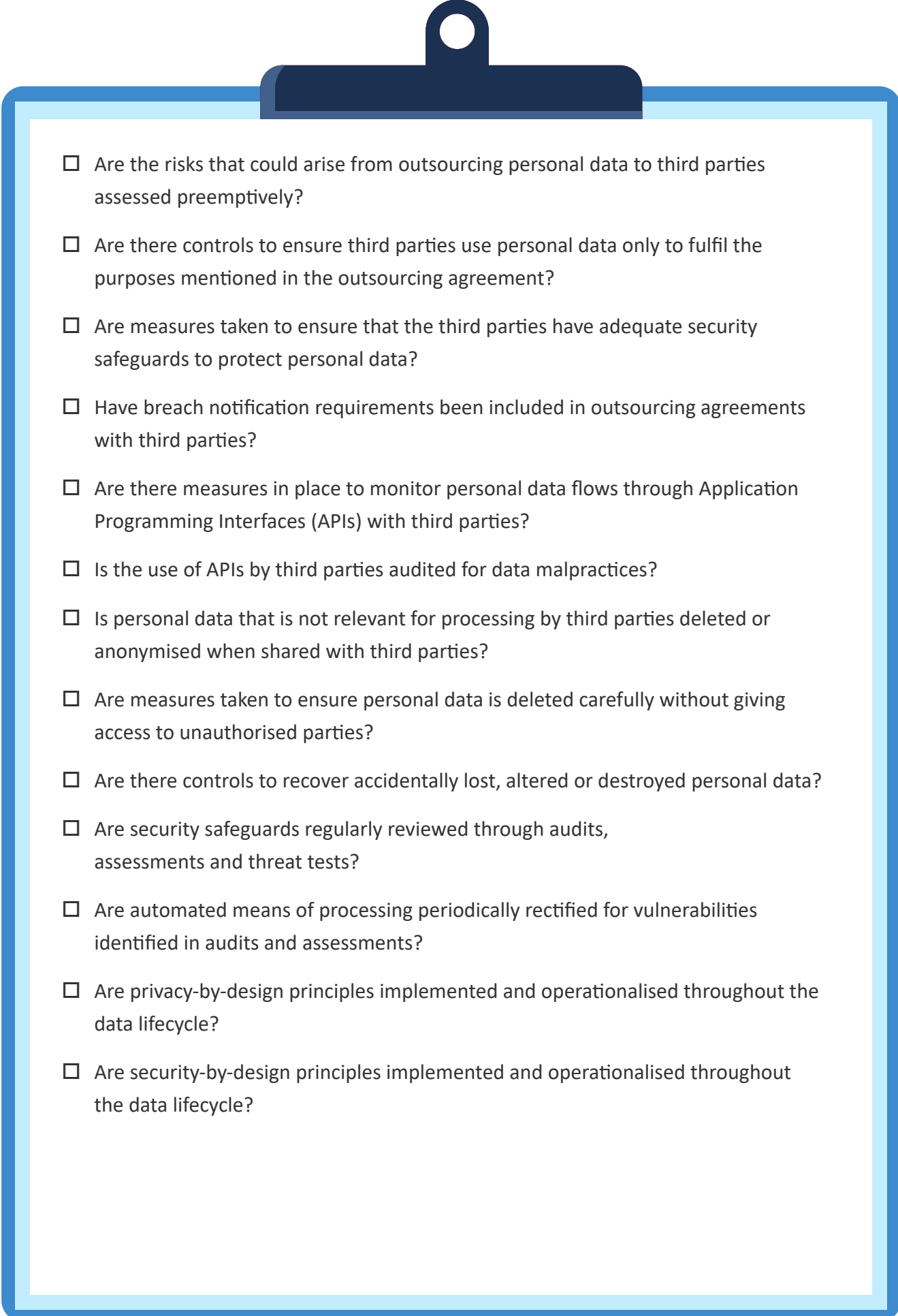
## COLLECTING ACCURATE AND PROPORTIONATE PERSONAL DATA FOR PROVIDING INSURANCE

- Is the personal data processed necessary for the purpose of processing?
- Is the personal data processed relevant for the purpose of processing?
- Is the data used for processing accurate, complete, representative, unbiased and up to date?
- Is unnecessary personal data deleted promptly?
- Is the personal data collected with the policyholders' consent?
- Is the personal data collected through lawful means?
- Is new personal data collected only when it is necessary for maintaining data accuracy or for fulfilling a purpose?
- Are Data Protection Impact Assessments (DPIA) conducted to ensure proportionate personal data in processed?
- Is the quality of personal data frequently assessed for processing?
- Are there mechanisms to filter incomplete, inaccurate, or unnecessary personal data during data collection?
- Are there protocols for assessing the quality of data collected from third parties?
- When using automated means, is the quality of outputs reviewed regularly when they are used for further processing activities?
- Are there measures to review the processing activities to identify and rectify the causes of bad data quality?
- Are there mechanisms to identify and rectify inaccuracies and alterations in personal data caused due to breach or cyberattack?
- Are records maintained of the source from which personal data was collected?
- Are records maintained of the measures taken to check the accuracy of data?
- Are records maintained of inaccuracies in personal data?
- Are records maintained of policyholders' challenges to the accuracy of personal data?



**PRINCIPLE 4:****SECURING POLICYHOLDERS' PERSONAL DATA**

- 
- Are information audits conducted to assess the inventory of the personal data?
  - Is the personal data inventory frequently revised and updated?
  - Are information audits conducted to understand vulnerabilities and risks to personal data?
  - Are risk assessments and threat tests conducted to understand risks to personal data?
  - Are the data protection impact assessments (DPIAs) and threat analyses conducted before using new technology for processing personal data?
  - Have anonymisation and de-identification techniques been implemented to secure personal data?
  - Are anonymised datasets reviewed continuously for the risk of reidentification?
  - Have technological measures, including encryption and passwords, been adopted for personal data protection?
  - Have organisational measures, including data access, data authentication and authorisation protocols, been adopted for personal data protection?
  - Have physical measures, including security clearances to personal data servers, been adopted for personal data protection?
  - Are data protection guarantees in the privacy notice operationalised through security safeguards?
  - Has a data breach and incident management process been established?
  - Does the data breach and incident management process help in addressing existing vulnerabilities and threats to personal data?
  - Does the data breach and incident management process enable policyholders to take steps to mitigate risks to personal data?

- 
- Are the risks that could arise from outsourcing personal data to third parties assessed preemptively?
  - Are there controls to ensure third parties use personal data only to fulfil the purposes mentioned in the outsourcing agreement?
  - Are measures taken to ensure that the third parties have adequate security safeguards to protect personal data?
  - Have breach notification requirements been included in outsourcing agreements with third parties?
  - Are there measures in place to monitor personal data flows through Application Programming Interfaces (APIs) with third parties?
  - Is the use of APIs by third parties audited for data malpractices?
  - Is personal data that is not relevant for processing by third parties deleted or anonymised when shared with third parties?
  - Are measures taken to ensure personal data is deleted carefully without giving access to unauthorised parties?
  - Are there controls to recover accidentally lost, altered or destroyed personal data?
  - Are security safeguards regularly reviewed through audits, assessments and threat tests?
  - Are automated means of processing periodically rectified for vulnerabilities identified in audits and assessments?
  - Are privacy-by-design principles implemented and operationalised throughout the data lifecycle?
  - Are security-by-design principles implemented and operationalised throughout the data lifecycle?



### PRINCIPLE 5:

## USING OR DISCLOSING PERSONAL DATA WITH THE CONSENT OF THE POLICYHOLDER

- Is a specific list of third parties to whom personal data may be disclosed maintained?
- Has the policyholder been provided with a standard list of third parties to whom personal data may be disclosed?
- Is a list of purposes for which personal data may be shared to third parties disclosed to policyholders?
- Have personal data disclosures to third parties stopped after policyholders have withdrawn consent?
- Have mechanisms been installed to receive and record data porting requests from policyholders?
- Are there organisation-level policies to recognise and operationalise data porting requests?
- Has capacity been developed in the organisation to recognise and operationalise data porting requests?
- Have measures been adopted to respond to porting requests in a timely manner?
- Has the identity of the requesting policyholder been verified before transmitting data?
- Have measures been adopted to receive and transmit personal data to third parties on policyholders' request?
- Can policyholders request for porting information at reasonable cost?
- Is personal data transmitted on policyholders' request without placing legal or technical obstacles?
- Is personal data transmitted on policyholders' request in a structured, commonly used and machine-readable format?
- Is personal data transmitted on policyholders' request in a secure method?
- Is the assessment of policyholder maintained distinctly from policyholders' personal data?




**PRINCIPLE 6:**

**ENABLING POLICYHOLDERS TO ACCESS AND RECTIFY THEIR PERSONAL DATA**

- Are personal data access and rectification processes clearly communicated to policyholders?
- Are policyholders able to access their own personal data in a structured, machine-readable format?
- Are policyholders able to access and rectify their personal data collected indirectly from third parties?
- Are policyholders able to access and rectify their personal data when they choose to without cost or delay?
- Do policyholders have the choice to rectify personal data through different physical and digital channels?
- Have changes been made to all personal data records to match the modifications made by policyholders?
- Have measures been taken to ensure that third parties rectify their personal data records?
- Have amended personal data records been provided to third parties after policyholders have made changes?


**PRINCIPLE 7:****USING AUTOMATED MEANS OF PROCESSING RESPONSIBLY**

- Are there measures to ensure transparency, accountability and explainability of decisions made by automated means?
- Can the factors and processes used by the automated means be explained in simple, clear and comprehensible terms to policyholders?
- Are there records of the actions taken to identify, document and mitigate risks from automated means to policyholders' rights?
- Are there records of the datasets and processes used by automated means to arrive at decisions?
- Have the automated means of processing been sandboxed or piloted to preemptively identify risks to policyholders?
- Are the automated means designed to be fit for the purpose of processing?
- Have the robustness and security of automated means been tested before being put into use?
- Have the reliability and accuracy of outputs produced by the automated means been tested before being put into use?
- Has it been demonstrated that the automated means of processing provide legitimate outputs without discrimination?
- Is the data being processed representative, unbiased and of high-quality?
- Has the personal data that is being processed by automated means been de-biased?
- Have the best standards been adopted for gathering and labelling personal data that will be used for processing by automated means?

- 
- Has bias in the decision-making process by automated means been identified and addressed?
  - Are automated means examined continually to identify vulnerabilities?
  - Have measures been adopted to mitigate the risks identified from automated means?
  - Are the personnel who develop and administrate automated means trained to ensure responsible processing?
  - Have policyholders been notified through all service delivery channels that automated means may be used for making decisions about them?
  - Are policyholders able to contest decisions made through automated means?
  - Are policyholders able to submit complaints about decisions made through automated means?
  - Are policyholders able to contest or seek review of decisions made through automated means?
  - Are policyholders able to seek redress when their rights are harmed by processing by automated means?
  - Do policyholders have access to data management tools that can help them review, edit, and update personal data that is processed through automated means?
  - Have policyholders been made aware of their rights about how their personal data is processed through automated means?

**PRINCIPLE 8:****DEMONSTRATING COMPLIANCE WITH BEST DATA PROTECTION PRACTICES**

- Are there protocols for the collection of personal data?
- Are there protocols for controlling access to personal data?
- Are there protocols for retaining and deleting personal data?
- Are there protocols for managing personal data breaches and other cyber incidents?
- Are there protocols for imparting data-privacy training to personnel?
- Are there data policies in place that define the means to ensure data quality?
- Are there data policies in place that define security safeguards?
- Are personnel trained to answer inquiries about privacy policies, consent processes, security safeguards and redressal processes?
- Are personnel appointed for monitoring compliance with data protection law and ensuring best practices in data protection?
- Are the names of personnel responsible for data protection practices published for policyholders' reference?
- Is there an effective, efficient, speedy and time-bound grievance redressal mechanism in place that can help policyholders resolve data-related grievances?
- Are the redressal mechanisms simple?
- Are policyholders able to seek redress through both digital and physical channels?
- Have redressal channels been leveraged to gain feedback directly from policyholders?
- Are audits conducted to assess the effectiveness of privacy notices, security safeguards and key data protection practices?

- 
- Have risk assessment frameworks for processing personal data been established?
  - Are third party service providers informed about past vulnerabilities and attacks?
  - Are records of the source from where personal data was collected maintained?
  - Are records of the measures taken to check accuracy of data maintained?
  - Are records of the processing activities that were undertaken with the personal data maintained?
  - Are records of the disclosure of personal data to third parties maintained?
  - Are records of the security safeguards installed maintained?



# References

- <sup>i</sup> D. Kessler et al., 'The Macroeconomic Role of Insurance', in *The Economics, Regulation and Systemic Risk of Insurance Markets*, (2017).
- <sup>ii</sup> Insurance Regulatory and Development Authority of India, Annual Report 2020-2021, <https://www.irdai.gov.in/admincms/cms/uploadedfiles/annual%20reports/Annual%20Report%202020-21.pdf>
- <sup>iii</sup> L. Brainard, 'What is the Role of Insurance in Economic Development?', Zurich Government Industry Affairs Thought Leadership series, (2008).
- <sup>iv</sup> OECD, *The Institutional Structure of Insurance Regulation and Supervision*, (2018), <https://www.oecd.org/finance/The-Institutional-Structure-of-Insurance-Regulation-and-Supervision.pdf>
- <sup>v</sup> F. Thouvenin et al., *Big Data in the Insurance Industry: Leeway and Limits for Individualising Insurance Contracts*, 10, 209, (2019), *JOURNAL OF INTELLECTUAL PROPERTY, INFORMATION TECHNOLOGY AND ELECTRONIC COMMERCE LAW*, [https://www.jipitec.eu/issues/jipitec-10-2-2019/4916/JIPITEC\\_10\\_2\\_2019\\_209\\_Thouvenin\\_Suter\\_George\\_and\\_Weber](https://www.jipitec.eu/issues/jipitec-10-2-2019/4916/JIPITEC_10_2_2019_209_Thouvenin_Suter_George_and_Weber)
- <sup>vi</sup> M.N. King et al, *Use of Big Data in Insurance*, in *The Palgrave Handbook of Technological Finance*, (2021).
- <sup>vii</sup> See, for example, Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015, [https://www.irdai.gov.in/admincms/cms/frmGeneral\\_Layout.aspx?page=PageNo2604&flag=1](https://www.irdai.gov.in/admincms/cms/frmGeneral_Layout.aspx?page=PageNo2604&flag=1)
- <sup>viii</sup> International Association of Insurance Supervisors, *FinTech Developments in the Insurance Industry*, INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS, (2017), <https://www.iaisweb.org/page/supervisory-material/other-supervisory-papers-and-reports/file/65440/report-on-fintech-developments-in-the-insurance-industry>
- <sup>ix</sup> International Association of Insurance Supervisors, *FinTech Developments in the Insurance Industry*, INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS, (2017), <https://www.iaisweb.org/page/supervisory-material/other-supervisory-papers-and-reports/file/65440/report-on-fintech-developments-in-the-insurance-industry>
- <sup>x</sup> KPMG. (n.d.), *The COVID-19 catalyst: Insurers race to digitize*, KPMG, (2020), <https://home.kpmg/xx/en/home/insights/2020/11/the-covid-19-catalyst-insurers-race-to-digitize.html>
- <sup>xi</sup> See, for example, C. Eckert, K. Osterrieder, *How digitalization affects insurance companies: overview and use cases of digital technologies*, *German Journal of Risk and Insurance*, (2020), <https://link.springer.com/article/10.1007/s12297-020-00475-9>
- <sup>xii</sup> OECD, *Technology and innovation in the insurance sector*, OECD, (2017), <https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf>
- <sup>xiii</sup> G. Cornelli et al, *Digging for gold: how regulatory sandboxes help fintech raise funding*, *VOX EU*, (2021), <https://voxeu.org/article/how-regulatory-sandboxes-help-fintechs-raise-funding>
- <sup>xiv</sup> OECD, *Technology and innovation in the insurance sector*, OECD, (2017), <https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf>
- <sup>xv</sup> D. Medine, F. Montes, *Data Protection and Privacy for Alternative Data*, *WORLD BANK AND CGAP*, (2018), [https://www.gpfi.org/sites/gpfi/files/documents/Data\\_Protection\\_and\\_Privacy\\_for\\_Alternative\\_Data\\_WBG.pdf](https://www.gpfi.org/sites/gpfi/files/documents/Data_Protection_and_Privacy_for_Alternative_Data_WBG.pdf)
- <sup>xvi</sup> T. Singhel, *Policyholders Protection with Digital Emphasis*, *IRDAI Journal*, (December 2019), <https://www.policyholder.gov.in/uploads/CEDocuments/December%202019.1.pdf>
- <sup>xvii</sup> Swiss Re Institute, 'World insurance: riding out the 2020 pandemic storm', *sigma* No 4/2020, SWISS RE INSTITUTE, (2020), <https://tinyurl.com/39ewdjus>.
- <sup>xviii</sup> Swiss Re Institute, 'World Insurance Series', SWISS RE INSTITUTE, (2021), <https://tinyurl.com/a3um87tz>.
- <sup>xix</sup> Lloyd's, *A world at risk: closing the Insurance Gap*, Lloyd's (2018), <https://assets.lloyds.com/assets/pdf-lloyds-underinsurance-report-final/1/pdf-lloyds-underinsurance-report-final.pdf>.
- <sup>xx</sup> Bandyopadhyay et al, *India's insurance sector: challenges and opportunities*, *IDEAS FOR INDIA* (2020), <https://www.ideasforindia.in/topics/money-finance/india-s-insurance-sector-challenges-and-opportunities.html>
- <sup>xxi</sup> G.N. Bajpai, *Why non-life insurance eludes the masses*, *THE HINDU BUSINESS LINE* (2019), <https://www.thehindubusinessline.com/opinion/why-non-life-insurance-eludes-the-masses/article26857093.ece>
- <sup>xxii</sup> Ray et al., 'India's insurance sector: challenges and opportunities', Working Paper 394, *INDIAN COUNCIL FOR RESEARCH ON INTERNATIONAL ECONOMIC RELATIONS*, (2020), [https://icrier.org/pdf/Working\\_Paper\\_394.pdf](https://icrier.org/pdf/Working_Paper_394.pdf); Patnaik et al, 'India needs more private insurance companies. Govt must use Covid trigger to make this happen', *THE PRINT*, (2021), <https://theprint.in/ilanomics/india-needs-more-private-insurance-companies-govt-must-use-covid-trigger-to-make-this-happen/705813/>
- <sup>xxiii</sup> K. Anurag, S. Rakesh, *Health Insurance for India's Missing Middle*, *NITI AAYOG*, (2021), [https://www.niti.gov.in/sites/default/files/2021-11/HealthInsuranceforIndia%E2%80%99sMissingMiddle\\_01-11-2021\\_digital%20pub.pdf](https://www.niti.gov.in/sites/default/files/2021-11/HealthInsuranceforIndia%E2%80%99sMissingMiddle_01-11-2021_digital%20pub.pdf)
- <sup>xxiv</sup> See the Marine Insurance Act, 1963.
- <sup>xxv</sup> See Emergency Risks (Undertakings) Insurance Act, 1971; Emergency Risks (Goods) Insurance Act, 1971.

<sup>xxvi</sup> See the Securities and Insurance Laws (Amendment and Validation) Act, 2012.

<sup>xxvii</sup> See the Actuaries Act of 2006.

<sup>xxviii</sup> See the Insurance Regulatory and Development Authority of India Act, 1999.

<sup>xxix</sup> S. Panda, Ir dai wants fuel pumps and cooking gas agencies to sell insurance, BUSINESS STANDARD, (2021), [https://www.business-standard.com/article/economy-policy/irdai-wants-fuel-pumps-and-cooking-gas-agencies-to-sell-insurance-121010801526\\_1.html](https://www.business-standard.com/article/economy-policy/irdai-wants-fuel-pumps-and-cooking-gas-agencies-to-sell-insurance-121010801526_1.html)

<sup>xxx</sup> PTI, India is second largest insurtech market in Asia Pacific, S&P Global says, ECONOMIC TIMES, (May 18, 2021), <https://economictimes.indiatimes.com/tech/startups/india-is-second-largest-insurtech-market-in-asia-pacific-sp-global-says/articleshow/82735254.cms>

<sup>xxxi</sup> A. Shah et al, India Insurtech Landscape and Trends, BOSTON CONSULTING GROUP, (February 2021), <https://web-assets.bcg.com/9e/50/a96580d94cf18041ec69c4473328/bcg-insurtech-report.pdf>

<sup>xxxii</sup> See IRDAI (Regulatory Sandbox) Regulations, 2019.

<sup>xxxiii</sup> Chauriye, N., Wearable Devices as Admissible Evidence: Technology is Killing Our Opportunity to Lie, (2016), <https://scholarship.law.edu/cgi/viewcontent.cgi?article=1018&context=jlt>

<sup>xxxiv</sup> Mint, Wearables, health apps can lower insurance premiums, Mint, (2018), <https://www.livemint.com/Technology/iNzsiCCh2aO7Khpam8ZFPm/Wearables-health-apps-can-lower-insurance-premiums.html>

<sup>xxxv</sup> BBC, John Hancock adds fitness tracking to all policies, BBC, (2018), <https://www.bbc.com/news/technology-45590293>; Aditya Birla Capital. (n.d.). TM Active Dayz supported activity tracking devices and apps, Aditya Birla Capital, <https://www.adityabirlacapital.com/healthinsurance/assets/pdf/supported-device-list.pdf>

<sup>xxxvi</sup> Bhargavi, R., & Arumugam, A survey on driving behavior analysis in usage based insurance using big data, <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0249-5#citeas>

<sup>xxxvii</sup> I.Tselentis, D., Yannis, G., & Vlahogianni, E. I., Innovative Insurance Schemes: Pay as/how You Drive, (2016) <https://reader.elsevier.com/reader/sd/pii/S2352146516300898?token=2143939D7795E7FF08D93435402E4A31A803151F3A4942027C2290BD2DC6E219927E6FE66B3F71317E6D3016EEE96F9F&originRegion=eu-west-1&originCreation=20211001092708>

<sup>xxxviii</sup> OECD, The Impact of Big Data and Artificial Intelligence in the Insurance Sector, (2020), <https://www.oecd.org/finance/Impact-Big-Data-AI-in-the-Insurance-Sector.pdf>

<sup>xxxix</sup> Information Commissioner's Office, 'Big Data, Artificial Intelligence, Machine Learning and Data Protection', INFORMATION COMMISSIONER'S OFFICE, (2017), <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>

<sup>xl</sup> A. Rao, Emerging Technologies in Insurance & Adoption Strategies by Various Stakeholders, IRDAI JOURNAL, (November 2020), <https://www.policyholder.gov.in/uploads/CEDocuments/IRDAI%20JOURNAL%20FINAL-compressed.pdf>

<sup>xli</sup> See A. Majumdar et. al., Competing in a new age of insurance: How India is adopting emerging technologies, PRICE WATERHOUSE COOPERS, (2019), <https://www.pwc.in/assets/pdfs/consulting/financial-services/competing-in-a-new-age-of-insurance.pdf>

<sup>xlii</sup> A. Singh, S. Prasad, Artificial Intelligence in Digital Credit in India, DVARA RESEARCH, (2020), <https://www.dvara.com/blog/2020/04/13/artificial-intelligence-in-digital-credit-in-india/>

<sup>xliii</sup> Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors, AIR 2017 SC 4161

<sup>xliv</sup> Joint Committee on the Personal Data Protection Bill, 2019, Report of the Joint Committee on the Personal Data Protection Bill, 2019, (December 16th 2021), [http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17\\_Joint\\_Committee\\_on\\_the\\_Personal\\_Data\\_Protection\\_Bill\\_2019\\_1.pdf](http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf)

<sup>xlv</sup> InsurTech Working Group, Report on InsurTech in the context of Risk Assessment, Product Design and Pricing, INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY OF INDIA, (2018), [https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral\\_Layout.aspx?page=PageNo3519&flag=1](https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3519&flag=1)

<sup>xlvi</sup> Section 2(1)(f), Insurance Regulatory and Development Authority of India Act, 1999, [https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral\\_Layout.aspx?page=PageNo108&flag=1](https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo108&flag=1); Regulation 2(d), Insurance Regulatory and Development Authority of India, (Payment of commission or remuneration or reward to insurance agents and insurance intermediaries) Regulations, 2016; [https://www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/Regulations/Consolidated/IRDAI\(Payment%20of%20Commission%20InsAgentsIntermediaries\)2016\\_Consolidated.pdf](https://www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/Regulations/Consolidated/IRDAI(Payment%20of%20Commission%20InsAgentsIntermediaries)2016_Consolidated.pdf) ;

<sup>xlvii</sup> Insurance Regulatory and Development Authority of India, Annual Report 2020-2021, <https://www.irdai.gov.in/admincms/cms/uploadedfiles/annual%20reports/Annual%20Report%202020-21.pdf>

<sup>xlviii</sup> K.N. Kalyani, One intermediary, many insurers, THE HINDU, (September 13th, 2020), <https://www.thehindu.com/business/one-intermediary-many-insurers/article32590208.ece>

<sup>xlix</sup> R. Venkatesan, Role of Intermediaries in Insurance Industry, IRDAI JOURNAL, 14, (2), (February 2016), <https://www.policyholder.gov.in/uploads/CEDocuments/February%20Journal%202016%20issue.pdf>

<sup>l</sup> IRDAI, Circular on Submission of Insurance Data to Insurance Information Bureau of India, (20th June 2013), <https://admin.iib.gov.in/uploads/CEDocuments/Mandate%20for%20Insurance%20data.pdf>

<sup>ll</sup> See, for example, RBI, 'Guidelines for Banks undertaking Insurance Broking and Agency Business', (2015), <https://www.rbi.org.in/Scripts/>

NotificationUser.aspx?Id=9489&Mode=0

<sup>liii</sup> D. Medine, F. Montes, Data Protection and Privacy for Alternative Data, WORLD BANK AND CGAP, (2018), [https://www.gpfi.org/sites/gpfi/files/documents/Data\\_Protection\\_and\\_Privacy\\_for\\_Alternative\\_Data\\_WBG.pdf](https://www.gpfi.org/sites/gpfi/files/documents/Data_Protection_and_Privacy_for_Alternative_Data_WBG.pdf)

<sup>liiii</sup> Information Commissioner's Office, Anonymisation: managing data protection risk code of practice, (2021), <https://ico.org.uk/media/1061/anonymisation-code.pdf>

<sup>liiv</sup> Information Commissioner's Office, What is automated individual decision-making and profiling?, (2018), <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling-1-1.pdf>

<sup>liv</sup> For more on the methodology of customer journey mapping as applied to the insurance sector, see A. Koning and G. Murthy, Customer Empowerment in Finance, Consultative Group to Assist the Poor (CGAP), Perspectives No. 3, August 2017 available at [https://www.cgap.org/sites/default/files/researches/documents/Perspective-Customer-Empowerment-in-Finance-Aug-2017\\_0.pdf](https://www.cgap.org/sites/default/files/researches/documents/Perspective-Customer-Empowerment-in-Finance-Aug-2017_0.pdf) (last accessed on October 22, 2021).

<sup>lvi</sup> See Swiss Re Ltd., Digital Distribution in Insurance, Sigma, No. 2/2014, March 31 2014, available at: <https://www.swissre.com/dam/jcr:ec0e233b-0656-4f58-b2ae-7245abacf1df/sigma2-2014-en.pdf> (last accessed on October 22, 2021); J. Poon et al, Human Behaviour and the Life Insurance Application Journey, Behavioural Economics in Action at Rotman, Research Report Series, October 17 2017, available at <https://www.rotman.utoronto.ca/-/media/Files/Programs-and-Areas/BEAR/White-Papers/BEAR-LifeInsurance.pdf?la=en> (last accessed on October 22, 2021);

<sup>lvii</sup> See IRDAI Press Release, Paperless KYC process through Aadhaar Authentication Services of UIDAI, (April 2020), [https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral\\_Layout.aspx?page=PageNo4109](https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo4109); IRDAI Circular, Video Based Identification Process, (September 2020), [https://www.irdai.gov.in/ADMINCMS/cms/whatsNew\\_Layout.aspx?page=PageNo4246&flag=1](https://www.irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo4246&flag=1)

<sup>lviii</sup> IRDAI Press Release, Paperless KYC process through Aadhaar Authentication Services of UIDAI, (April 2020), [https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral\\_Layout.aspx?page=PageNo4109](https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo4109); IRDAI Circular, Video Based Identification Process, (September 2020), [https://www.irdai.gov.in/ADMINCMS/cms/whatsNew\\_Layout.aspx?page=PageNo4246&flag=1](https://www.irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo4246&flag=1)

<sup>lix</sup> IRDAI, Revised guidelines on insurance repositories and electronic issuance of insurance policies, (May 2015), <https://www.policyholder.gov.in/uploads/CEDocuments/Revised%20Guidelines%202019-05-15%20on%20Insurance%20Repositories.PDF>

<sup>lx</sup> Bishnu, I. & Aakulu, S., Data Protection in the Indian Insurance Sector – Regulatory Framework Part I, INDIAN CORPORATE LAW (13 May 2019), <https://corporate.cyrilamarchandblogs.com/2019/05/data-protection-indian-insurance-sector-regulatory-framework-part-1/>; Bishnu, I. & Aakulu, S., Data Protection in the Indian Insurance Sector – Regulatory Framework Part II, INDIAN CORPORATE LAW (14 May 2019), <https://corporate.cyrilamarchandblogs.com/2019/05/data-protection-indian-insurance-sector-regulatory-framework-part-2/>.

<sup>lxi</sup> See, for instance, Sections 43A of the Infotech Act; Chapter VII, Aadhaar Act.

<sup>lxii</sup> See Sections 19 and 20, CIRC Act.

<sup>lxiii</sup> See IRDAI (Maintenance of Insurance Records) Regulations, 2015; IRDAI (Minimum Information Required for Investigation and Inspection) Regulations, 2020; IRDAI (Protection of Policyholders' Interests) Regulations, 2017; IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017; IRDAI Guidelines on Information and Cybersecurity for Insurers, 2017.

<sup>lxiv</sup> See IRDAI (Insurance Brokers) Regulations, 2018.

<sup>lxv</sup> See IRDAI (Insurance Web Aggregators) Regulations, 2017

<sup>lxvi</sup> See IRDAI (Registration of Corporate Agents) Regulations, 2015

<sup>lxvii</sup> See IRDAI (Insurance Services by Common Public Service Centres) Regulations, 2019

<sup>lxviii</sup> See IRDAI (Insurance Surveyors and Loss Assessors) Regulations, 2015

<sup>lxix</sup> See IRDAI Guidelines on Insurance Repositories and electronic issuance of Insurance Policies, 2015.

<sup>lxx</sup> See IRDAI (Third Party Administrators - Health Services) Regulations, 2016.

<sup>lxxi</sup> See IRDAI Guidelines on Insurance e-Commerce, 2017s

<sup>lxxii</sup> See M.F. Vidal, D. Medine, Is Data Privacy Good for Business?, Consultative Group to Assist the Poor, (2019) [https://www.cgap.org/sites/default/files/publications/2019\\_12\\_Focus\\_Note\\_Is\\_Data\\_Privacy\\_Good\\_for\\_Business\\_1.pdf](https://www.cgap.org/sites/default/files/publications/2019_12_Focus_Note_Is_Data_Privacy_Good_for_Business_1.pdf)

<sup>lxxiii</sup> See M.F. Vidal, D. Medine, Is Data Privacy Good for Business?, Consultative Group to Assist the Poor, (2019) [https://www.cgap.org/sites/default/files/publications/2019\\_12\\_Focus\\_Note\\_Is\\_Data\\_Privacy\\_Good\\_for\\_Business\\_1.pdf](https://www.cgap.org/sites/default/files/publications/2019_12_Focus_Note_Is_Data_Privacy_Good_for_Business_1.pdf)

<sup>lxxiv</sup> Burman, A. & Rai, S., What is India's Sweeping Personal Data Protection Bill?, CARNEGIE INDIA (9 March 2020), <https://carnegieindia.org/2020/03/09/what-is-in-india-s-sweeping-personal-data-protection-bill-pub-80985>.

<sup>lxxv</sup> Greenleaf, G. & Cottier, B., 2020 Ends a Decade of 62 New Data Privacy Laws, 163 Privacy Laws & Business International Report, 24-26 2020, retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3572611](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611); The Data Protection Bill, 2021, 17\_Joint\_Committee\_on\_the\_Personal\_Data\_Protection\_Bill\_2019\_1.pdf.

<sup>lxxvi</sup> A. Manikandan, Alternative data can gauge creditworthiness, if law permits, ECONOMIC TIMES, (2019), <https://economictimes.indiatimes.com/markets/stocks/news/alternative-data-can-gauge-creditworthiness-if-law-permits/articleshow/68748552.cms>

<sup>lxxvii</sup> United India Insurance Company Ltd v. Jai Prakash Tayal, (2018) SCC OnLine Del 7415; para 87.

- <sup>boxxviii</sup> United India Insurance Company Ltd. v. Jay Parkash Tayal, (2020) 15 SCC 115; para 4.
- <sup>boxxix</sup> IAIS, Issues Paper on Increasing Digitalisation in Insurance and its Potential Impact on Consumer Outcomes, IAIS (November 2018), retrieved from <https://www.iaisweb.org/page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-insurance-and-its-potential-impact-on-consumer-outcomes>.
- <sup>boxxx</sup> IAIS, Issues Paper on the Use of Big Data Analytics in Insurance, IAIS (26 February 2020), retrieved from <https://www.iaisweb.org/page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-insurance-and-its-potential-impact-on-consumer-outcomes>.
- <sup>boxxxi</sup> IRDAI, Annual Report 2019-20, IRDAI (10 February 2021), , [https://www.irdai.gov.in/admincms/cms/uploadedfiles/annual%20reports/IRDAI%20Annual%20Report%202019-20\\_English.pdf](https://www.irdai.gov.in/admincms/cms/uploadedfiles/annual%20reports/IRDAI%20Annual%20Report%202019-20_English.pdf),
- <sup>boxxxii</sup> See M. Boyd, Digital Finance APIs Come with Risks – Here’s One Way to Manage Them, CONSULTATIVE GROUP TO ASSIST THE POOR, (2020), <https://www.cgap.org/blog/digital-finance-apis-come-risks-heres-one-way-manage-them>
- <sup>boxxxiii</sup> See IRDA, Guidelines on Migration and Portability of health insurance policies, IRDA, (2020), [https://www.irdai.gov.in/ADMINCMS/cms/frmGuidelines\\_Layout.aspx?page=PageNo3987](https://www.irdai.gov.in/ADMINCMS/cms/frmGuidelines_Layout.aspx?page=PageNo3987).
- <sup>boxxxiv</sup> See A. Singh, S. Prasad, Artificial Intelligence in Digital Credit in India, DVARA RESEARCH, (2020), <https://www.dvara.com/blog/2020/04/13/artificial-intelligence-in-digital-credit-in-india/>
- <sup>boxxxv</sup> GSMA, Protecting Privacy and Data in the Internet of Things, GSMA, (2019) <https://www.gsma.com/iot/wp-content/uploads/2019/06/Protecting-Privacy-big-data-report-gsma.pdf>
- <sup>boxxxvi</sup> NAIC, Telematics/Usage-Based Insurance, Naic, (2021), [https://content.naic.org/cipr\\_topics/topic\\_telematicsusagebased\\_insurance.htm](https://content.naic.org/cipr_topics/topic_telematicsusagebased_insurance.htm)
- <sup>boxxxvii</sup> Minty, D., Do personalised premiums mean the end of risk pooling?, Ethics and Insurance, (2013), <https://ethicsandinsurance.info/2013/04/30/personalised-premiums-risk-pooling/>
- <sup>boxxxviii</sup> Wallace, M., Revealed - Key findings from the FCA’s sector views report, (2018), <https://www.insurancebusinessmag.com/uk/news/breaking-news/revealed--key-findings-from-the-fcas-sector-views-report-214089.aspx>
- <sup>boxxxix</sup> Fallow, B., Tarumi, T., & Tanaka, H., Influence of skin type and wavelength on light wave reflectance, (2013), <https://link.springer.com/article/10.1007/s10877-013-9436-7>
- <sup>xc</sup> Fuller, D., Reliability and Validity of Commercially Available Wearable Devices for Measuring Steps, Energy Expenditure, and Heart Rate: Systematic Review, (2020), <https://mhealth.jmir.org/2020/9/e18694/citations> ; Moço, A. V., Stuijk, S., & de Haan, G., Skin inhomogeneity as a source of error in remote PPG-imaging, (2016), <https://www.osapublishing.org/boe/fulltext.cfm?uri=boe-7-11-4718&id=353258>
- <sup>xc<sup>i</sup></sup> Notice is also a key provision in Clause 7 of the upcoming Data Protection Bill, 2021.
- <sup>xc<sup>ii</sup></sup> IAIS, Issues Paper on the Use of Big Data Analytics in Insurance, IAIS (26 February 2020), retrieved from <https://www.iaisweb.org/page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-insurance-and-its-potential-impact-on-consumer-outcomes>; Kim, Y., Wang, Q and Roh, T., Do information and service quality affect perceived privacy protection, satisfaction, and loyalty? Evidence from a Chinese O2O-based mobile shopping application. 101483 Telematics and Informatics, (2020) retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0736585320301428>; Bleier, A., Goldfrab, A. & Tucker, C., Consumer privacy and the future of data-based innovation and marketing, International Journal of Research in Marketing, (2020), retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0167811620300331>.
- <sup>xc<sup>iii</sup></sup> Susser, D., Notice After Notice-and-Consent: Why Privacy Disclosures are Valuable Even if Consent Frameworks Aren’t, 9 Journal of Information Policy, 148-173 (2019); Kim, Y., Wang, Q and Roh, T., Do information and service quality affect perceived privacy protection, satisfaction, and loyalty? Evidence from a Chinese O2O-based mobile shopping application. 101483 Telematics and Informatics, (2020) retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0736585320301428>; Bleier, A., Goldfrab, A. & Tucker, C., Consumer privacy and the future of data-based innovation and marketing, International Journal of Research in Marketing, (2020), retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0167811620300331>.
- <sup>xc<sup>iv</sup></sup> Notice is a key provision in clause 7 of the upcoming Personal Data Protection Bill, 2019.
- <sup>xc<sup>v</sup></sup> Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (February 2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en>.
- <sup>xc<sup>vi</sup></sup> Thompson, K. & Stockburger P., Data protection & consent: Comparing and contrasting changes to American and Canadian privacy laws, LEXPERT (May 2021), <https://www.lexpert.ca/legal-insights/data-protection-consent-comparing-and-contrasting-changes-to-american-and-canadian-privacy-laws/356250>.
- <sup>xc<sup>vii</sup></sup> Data Protection Bill, 2021,17\_Joint\_Committee\_on\_the\_Personal\_Data\_Protection\_Bill\_2019\_1.pdf; Dvara Research, The Data Protection Bill, 2018, DVARA RESEARCH (2017), <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>; General Data Protection Regulation, Art. 13 GDPR Information to be provided where personal data are collected from the data subject, GDPR (2016), <https://gdpr-info.eu/art-13-gdpr/>; Personal Data Protection Act, 2012, <https://sso.agc.gov.sg/Act/PDPA2012?Provids=legis#legis>; DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.
- <sup>xc<sup>viii</sup></sup> Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (February 2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en>.

- <sup>xcix</sup> UK Information Commissioner's Office, Consent, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>.
- <sup>c</sup> Data Protection Bill, 2021, 17\_Joint\_Committee\_on\_the\_Personal\_Data\_Protection\_Bill\_2019\_1.pdf; Dvara Research, The Data Protection Bill, 2018, DVARA RESEARCH (2018), <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>; General Data Protection Regulation, Art. 13 GDPR Information to be provided where personal data are collected from the data subject, GDPR (2016), <https://gdpr-info.eu/art-13-gdpr/>; Personal Data Protection Act, 2012, <https://sso.agc.gov.sg/Act/PDPA2012?Provlds=legis#legis>; DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.
- <sup>ci</sup> Calo, R., Against Notice Skepticism in Privacy (And Elsewhere), STANFORD CENTER FOR INTERNET AND SOCIETY (2011), <http://cyberlaw.stanford.edu/files/publication/files/ssrn-id1790144.pdf>; Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (February 2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en>; Solove, D.J., Privacy Self-Management and the Consent Dilemma, 126 Harvard Law Review, 1880 (2013), [https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2093&context=faculty\\_publications](https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2093&context=faculty_publications); Gilbert, A., California Consumer Privacy Act (CCPA) compliance guide: Everything you need to know, OSANO (19 August 2021), <https://www.osano.com/articles/ccpa-guide>.
- <sup>cii</sup> Fjeld, J. et.al, Principles Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, BERKMAN KLEIN CENTRE FOR INTERNET AND SOCIETY (2020), [https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final\\_v3.pdf?sequence=1&isAllowed=y](https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y); House of Commons Canada, Bill C-11, PARLIAMENT OF CANADA (November 2020), <https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading>.
- <sup>ciii</sup> UK Information Commissioner's Office, Why is consent important?, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/why-is-consent-important/>.
- <sup>civ</sup> UK Information Commissioner's Office, Why is consent important?, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/why-is-consent-important/>; CGAP, Dalberg & Dvara Research, Privacy on the Line: What people in India think about their data protection and privacy, DVARA RESEARCH (2017), <https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf>; Bleier, A., Goldfrab, A. & Tucker, C., Consumer privacy and the future of data-based innovation and marketing, International Journal of Research in Marketing, (2020), retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0167811620300331>.
- <sup>cv</sup> Notice is a key provision in clause 7 of the upcoming Personal Data Protection Bill, 2019.
- \* Notice is a key provision in clause 7 of the upcoming Data Protection Bill, 2021.
- <sup>cvi</sup> Reserve Bank of India, Directions regarding Registration and Operations of NBFC – Account Aggregators under section 45-IA of the Reserve Bank of India Act, 1934, RESERVE BANK OF INDIA (2021) [https://www.rbi.org.in/Scripts/bs\\_viewcontent.aspx?Id=3142](https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3142); The Data Protection Bill, 2021, clause 23(5), 17\_Joint\_Committee\_on\_the\_Personal\_Data\_Protection\_Bill\_2019\_1.pdf
- <sup>cvi</sup> Morey T., Forbath T., Schoop A., Customer Data: Designing for Transparency and Trust, Harvard Business Review (May 2015), <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>; Pacific Private Sector Development Initiative, Digital Financial Services in the Pacific: Experiences and Regulatory Issues, ASIAN DEVELOPMENT BANK (March 2016), <https://www.adb.org/publications/digital-financial-services-pacific>; Dvara Research, Dalberg & CGAP, Privacy on the Line: What people in India think about their data protection and privacy, DVARA RESEARCH (2017), <https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf>.
- <sup>cvi</sup> Fjeld, J. et.al, Principles Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, BERKMAN KLEIN CENTRE FOR INTERNET AND SOCIETY (2020), [https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final\\_v3.pdf?sequence=1&isAllowed=y](https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y).
- <sup>cix</sup> Office of the Privacy Commissioner of Canada, Accuracy, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (May 2013), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations\\_04\\_accuracy/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_04_accuracy/); UK Information Commissioner's Office, Controllers checklist, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/controllers-checklist/>.
- <sup>cx</sup> UK Information Commissioner's Office, Consent, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>.
- <sup>cx</sup> DSCI, Sectoral Privacy Guide: Healthcare, DSCI (August 2021), retrieved from <https://www.dsci.in/sectoral-privacy-project/healthcare-sector/>; Dvara Research, Comments to the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 introduced in the Lok Sabha on 11 December 2019, DVARA RESEARCH (March 2020), <https://www.dvara.com/research/wp-content/uploads/2020/03/Dvara-Research-Final-Submission-Comments-to-the-Joint-Parliamentary-Committee-on-PDP-Bill.pdf>.
- <sup>cxii</sup> Dvara Research, Comments to the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 introduced in the Lok Sabha on 11 December 2019, DVARA RESEARCH (March 2020), <https://www.dvara.com/research/wp-content/uploads/2020/03/Dvara-Research-Final-Submission-Comments-to-the-Joint-Parliamentary-Committee-on-PDP-Bill.pdf>; UK Information Commissioner's Office, Consent, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>.
- <sup>cxiii</sup> UK Information Commissioner's Office, Consent, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>.
- <sup>cxiv</sup> IAIS, Issues Paper on the Use of Big Data Analytics in Insurance, IAIS (26 February 2020), retrieved from <https://www.iaisweb.org/>

page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-insurance-and-its-potential-impact-on-consumer-outcomes.

<sup>cxv</sup> Ibid.

<sup>cxvi</sup> Proportionate data collection and data quality are key provisions in clauses 6 and 8 of the upcoming Personal Data Protection Bill, 2019, respectively.

<sup>cxvii</sup> The Data Protection Bill, 2021, 17\_Joint\_Committee\_on\_the\_Personal\_Data\_Protection\_Bill\_2019\_1.pdf; Dvara Research, The Data Protection Bill, 2018, DVARA RESEARCH (2018), <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>; General Data Protection Regulation, Art. 13 GDPR Information to be provided where personal data are collected from the data subject, GDPR (2016), <https://gdpr-info.eu/art-13-gdpr/>; Personal Data Protection Act, 2012, <https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=legis#legis>; DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.

<sup>cxviii</sup> Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 6 – Accuracy, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_accuracy/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accuracy/); The Royal Borough of Kensington and Chelsea, A Framework for better quality data and performance information, THE ROYAL BOROUGH OF KENSINGTON AND CHELSEA (2010), <https://www.rbkc.gov.uk/PDF/Data%20Quality%20Framework%20March%202010.pdf>.

<sup>cxix</sup> OAIC, Chapter 10: APP 10 – Quality of personal information, OAIC (2019), <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-10-app-10-quality-of-personal-information/>.

<sup>cxx</sup> DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.

<sup>cxxi</sup> Office on the Privacy Commissioner of Canada, Accuracy, OFFICE ON THE PRIVACY COMMISSIONER OF CANADA (2013), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations\\_04\\_accuracy/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_04_accuracy/).

<sup>cxixii</sup> Monetary Authority of Singapore, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, 2019, MONETARY AUTHORITY OF SINGAPORE (7 February 2019), <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/FEAT-Principles-Updated-7-Feb-19.pdf>.

<sup>cxixiii</sup> ISO, Data quality – Part 61: Data quality management: Process reference model, ISO (2016), <https://www.sis.se/api/document/preview/921215/>; Leo, L. et.al, Data Quality Assessment, 45 Communications of the ACM, 4 (2002), <http://web.mit.edu/tdqm/www/tdqmpub/PipinoLeeWangCACMApr02.pdf>; Batini, C. et.al, A Framework and a Methodology for Data Quality Assessment and Monitoring, MASSACHUSETTS INSTITUTE OF TECHNOLOGY (2007), <http://mitiq.mit.edu/iciq/pdf/a%20framework%20and%20a%20methodology%20for%20data%20quality%20assessment%20and%20monitoring.pdf>.

<sup>cxixiv</sup> DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.

<sup>cxixv</sup> UK Information Commissioner's Office, Principle (d): Accuracy, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>.

<sup>cxixvi</sup> Ibid.

<sup>cxixvii</sup> UK Information Commissioner's Office, Principle (d): Accuracy, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>; OAIC, Chapter 10: APP 10 – Quality of personal information, OAIC (2019), <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-10-app-10-quality-of-personal-information/>.

<sup>cxixviii</sup> IAIS, Issues Paper on the Use of Big Data Analytics in Insurance, IAIS (26 February 2020), retrieved from <https://www.iaisweb.org/page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-insurance-and-its-potential-impact-on-consumer-outcomes>.

<sup>cxixix</sup> The obligation on providers to adopt security safeguards is a key provision in clause 23 of the upcoming Personal Data Protection Bill, 2019.

\* The obligation on providers to adopt security safeguards is a key provision in clause 24 of the upcoming Data Protection Bill, 2021.

<sup>cxixxx</sup> UK Information Commissioner's Office, Controllers checklist, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/controllers-checklist/>.

<sup>cxixxxi</sup> IRDAI, Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, 2017, <https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf>; Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 1 – Accountability, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (August 2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_accountability/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/).

<sup>cxixxxii</sup> Data Protection Commission, Guidance Note: Guidance on Anonymisation and Pseudonymisation, DATA PROTECTION COMMISSION (June 2019), <https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf>.

<sup>cxixxxiii</sup> DSCI, Sectoral Privacy Guide: Healthcare, DSCI (August 2021), retrieved from <https://www.dsci.in/sectoral-privacy-project/healthcare-sector/>.

<sup>cxixxxiv</sup> PIPEDA, Personal Information Protection and Electronic Documents Act, 2019, <https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf>; Federal

Trade Commission, Protecting Personal Information, FEDERAL TRADE COMMISSION (2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf); Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 5 – Limiting use, disclosure and retention, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_use/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_use/); MasterCard, The Global Data Responsibility Imperative, MASTERCARD (October 2019), <https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/global-data-responsibility-whitepaper-customer-10232019.pdf>.

<sup>xxxv</sup> PIPEDA, Personal Information Protection and Electronic Documents Act, 2019, <https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf>; Federal Trade Commission, Protecting Personal Information, FEDERAL TRADE COMMISSION (2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf); Personal Data Protection Commission, Guide to securing personal data in electronic medium, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2017), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/OtherGuides/guidetosecuringpersonaldatainelectronicmedium0903178d4749c8844062038829ff0000d98b0f.pdf?la=en>; MasterCard, The Global Data Responsibility Imperative, MASTERCARD (October 2019), <https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/global-data-responsibility-whitepaper-customer-10232019.pdf>.

<sup>xxxvi</sup> PIPEDA, Personal Information Protection and Electronic Documents Act, 2019, <https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf>; Federal Trade Commission, Protecting Personal Information, FEDERAL TRADE COMMISSION (2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf); Federal Trade Commission, Start With Security, FEDERAL TRADE COMMISSION (2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>; MasterCard, The Global Data Responsibility Imperative, MASTERCARD (October 2019), <https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/global-data-responsibility-whitepaper-customer-10232019.pdf>.

<sup>xxxvii</sup> Federal Trade Commission, Protecting Personal Information, FEDERAL TRADE COMMISSION (2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf); PIPEDA, Personal Information Protection and Electronic Documents Act, 2019, <https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf>.

<sup>xxxviii</sup> Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 7 – Safeguards, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_safeguards/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_safeguards/).

<sup>xxxix</sup> PIPEDA, Personal Information Protection and Electronic Documents Act, 2019, <https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf>.

<sup>cxl</sup> Personal Data Protection Commission, Guide To Securing Personal Data In Electronic Medium, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2015), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guidetosecuringpersonaldatainelectronicmedium0903178d4749c8844062038829ff0000d98b0f.pdf?la=en>.

<sup>cxli</sup> Fjeld, J. et.al, Principles Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, BERKMAN KLEIN CENTRE FOR INTERNET AND SOCIETY (2020), [https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final\\_v3.pdf?sequence=1&isAllowed=y](https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y).

<sup>cxlii</sup> UK Information Commissioner’s Office, Security, UK INFORMATION COMMISSIONER’S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>; Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 5 – Limiting use, disclosure and retention, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_use/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_use/).

<sup>cxliii</sup> IRDAI, Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, 2017, <https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf>; Dvara Research, The Dvara Data Protection Bill, 2018, DVARA RESEARCH (7 February 2018), <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>.

<sup>i</sup> Privacy-by-design espouses seven foundational principles which guide providers in embedding privacy in the systems, standards, protocols and processes of providers. See A. Cavoukian, Privacy by Design: the 7 Foundational Principles, (2009), INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, (August 2009), <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>

<sup>ii</sup> Security-by-design espouses principles for enabling and protecting data activities and assets against unauthorised access, use, disclosure, disruption, modification or destruction. The principles aim to maintain the integrity, confidentiality and availability of data. See here.

<sup>cxliv</sup> Ibid.

<sup>cxlv</sup> Ibid.

<sup>cxlvi</sup> Dvara Research, The Data Protection Bill, 2018, DVARA RESEARCH (7 February 2018), <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>.

<sup>cxlvii</sup> Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, EUROPEAN COMMISSION, (2 April 2013), retrieved from [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf).

<sup>cxlviii</sup> The Personal Data Protection Bill, 2019, cl.19(2), [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf)

<sup>cxlix</sup> Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, EUROPEAN COMMISSION, (2 April 2013), retrieved from [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf).

<sup>cl</sup> Purpose limitation and consent are key provisions in clauses 5 and 11 of the upcoming Personal Data Protection Bill, 2019.

<sup>cli</sup> DSCI, Sectoral Privacy Guide: Healthcare, DSCI (August 2021), retrieved from <https://www.dsci.in/sectoral-privacy-project/healthcare-sector/>; Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal data Protection Act, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2021), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en>; GDPR, Article 14 - Information to be provided where personal data have not been obtained from the data subject, gdpr-info.eu: <https://gdpr-info.eu/art-14-gdpr/>.

<sup>clii</sup> Dvara Research, Dvara Data Protection Bill, 2018 - Cl.11(6), DVARA RESEARCH (7 February 2018) <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>; UK Information Commissioner's Office, Right to data portability, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/>; UK Information Commissioner's Office, Right to data portability, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/>; Su, G., Singapore's PDPA's data portability obligation: Learning from the GDPR experience, WITHERS WORLDWIDE (3 February 2021), <https://www.withersworldwide.com/en-gb/insight/singapore-s-pdpa-s-data-portability-obligation-learning-from-the-gdpr-experience>; Su, G., Singapore's PDPA's data portability obligation: Learning from the GDPR experience, WITHERS WORLDWIDE (3 February 2021), <https://www.withersworldwide.com/en-gb/insight/singapore-s-pdpa-s-data-portability-obligation-learning-from-the-gdpr-experience>.

<sup>cliii</sup> UK Information Commissioner's Office, Principle (d): Accuracy, UK INFORMATION COMMISSIONER'S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>.

<sup>cliv</sup> Bleier, A., Goldfrab, A. & Tuckerc, C., Consumer privacy and the future of data-based innovation and marketing, International Journal of Research in Marketing, (2020), retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0167811620300331>.

<sup>clv</sup> Kim, Y., Wang, Q and Roh, T., Do information and service quality affect perceived privacy protection, satisfaction, and loyalty? Evidence from a Chinese O2O-based mobile shopping application. 101483 Telematics and Informatics, (2020) retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0736585320301428>; Bleier, A., Goldfrab, A. & Tuckerc, C., Consumer privacy and the future of data-based innovation and marketing, International Journal of Research in Marketing, (2020), retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0167811620300331>.

<sup>clvi</sup> The right to confirmation, access, correction and erasure are key provisions in clauses 17 and 18 of the upcoming Personal Data Protection Bill, 2019 will creates a similar obligation for providers.

\* The right to confirmation, access, correction and erasure are key provisions in clauses 17 and 18 of the upcoming Data Protection Bill, 2021 will create a similar obligation for providers.

<sup>clvii</sup> DSCI, Sectoral Privacy Guide: Healthcare, DSCI (August 2021), retrieved from <https://www.dsci.in/sectoral-privacy-project/healthcare-sector/>; The Data Protection Bill, 2021, clauses 18, 19 and 21, 17\_Joint\_Committee\_on\_the\_Personal\_Data\_Protection\_Bill\_2019\_1.pdf

<sup>clviii</sup> Personal Data Protection Commission, Advisory Guidelines On Key Concepts In the PDPA, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2019), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Chapter-15-9-Oct-2019.pdf>.

<sup>clix</sup> DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.

<sup>clx</sup> Office of the Privacy Commissioner of Canada, Accuracy, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (May 2013), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations\\_04\\_accuracy/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_04_accuracy/).

<sup>clxi</sup> Personal Data Protection Commission, Advisory Guidelines On Key Concepts In the PDPA, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2019), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Chapter-15-9-Oct-2019.pdf>.

<sup>clxii</sup> Office of the Privacy Commissioner of Canada, Accuracy, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (May 2013), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations\\_04\\_accuracy/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_04_accuracy/).

<sup>clxiii</sup> Personal Data Protection Commission, Advisory Guidelines On Key Concepts In the PDPA, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2019), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Chapter-15-9-Oct-2019.pdf>.

<sup>clxiv</sup> The Data Protection Bill, 2021, clause 17, 17\_Joint\_Committee\_on\_the\_Personal\_Data\_Protection\_Bill\_2019\_1.pdf

<sup>clxv</sup> GDPR, Right of Access, <https://gdpr-info.eu/issues/right-of-access/>

<sup>clxvi</sup> GDPR, Right of Access, <https://gdpr-info.eu/issues/right-of-access/>.

<sup>clxvii</sup> Dvara Research, The Dvara Data Protection Bill, 2018, DVARA RESEARCH (7 February 2018), Retrieved from <https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf>.

<sup>clxviii</sup> Personal Data Protection Commission, Advisory Guidelines On Key Concepts In the PDPA, SINGAPORE PERSONAL DATA PROTECTION COMMISSION (2019), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Chapter-15-9-Oct-2019.pdf>.

<sup>clxix</sup> IAIS, Issues Paper on the Use of Big Data Analytics in Insurance, IAIS (26 February 2020), retrieved from <https://www.iaisweb.org/page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-insurance-and-its-potential-impact-on-consumer-outcomes>; IAIS, Issues Paper on Increasing Digitalisation in Insurance and its Potential Impact on Consumer Outcomes, IAIS (November 2018), retrieved from <https://www.iaisweb.org/page/supervisory-material/issues-papers/file/77816/issues-paper-on-increasing-digitalisation-in-insurance-and-its-potential-impact-on-consumer-outcomes>.

<sup>clxx</sup> Fjeld, J. et.al., Principles Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, BERKMAN KLEIN CENTRE FOR INTERNET AND SOCIETY (2020), [https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final\\_v3.pdf?sequence=1&isAllowed=y](https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y).

<sup>clxxi</sup> Superintendency of Industry and Commerce, Colombia, Sandbox on Privacy by Design and Default in AI, OECD (2020), <https://stip.oecd.org/stip/policy-initiatives/2019%2Fdata%2FpolicyInitiatives%2F26973>; Norwegian Data Protection Authority, Framework for the



Regulatory Sandbox, DATATILSYNET (13 January 2021), <https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/framework-for-the-regulatory-sandbox/?print=true>; Global Privacy Assembly, Adopted Resolution on Accountability in the Development and Use of Artificial Intelligence, GLOBAL PRIVACY ASSEMBLY (2020), <https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN-1.pdf>; European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, EUROPEAN COMMISSION (2020), [https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf); High-level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, EUROPEAN COMMISSION (April 8 2019), retrieved from European Commission: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>; Dvara Research, Response dated 15 January 2021 to the Working Document: Enforcement Mechanisms for Responsible #AIforAll released by the NITI Aayog in November 2020, DVARA RESEARCH (18 January 2021), <https://www.dvara.com/research/wp-content/uploads/2021/01/Our-Response-to-the-Working-Document-on-Enforcement-Mechanisms-for-Responsible-AIforAll.pdf>.

cbxxii The Government of Canada, Directive on Automated Decision Making, THE GOVERNMENT OF CANADA (5 February 2019), <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>.

cbxxiii UK Information Commissioner’s Office, Rights related to automated decision making including profiling, UK INFORMATION COMMISSIONER’S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>; General Data Protection Regulation, 2016, art. 22, <https://gdpr-info.eu/art-22-gdpr/>.

cbxxiv Access Now, Human Rights in the Age of Artificial Intelligence, ACCESS NOW (November 2018), <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>; Monetary Authority of Singapore, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector, 2019, MONETARY AUTHORITY OF SINGAPORE (7 February 2019), <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/FEAT-Principles-Updated-7-Feb-19.pdf>.

cbxxv Monetary Authority of Singapore, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector, 2019, MONETARY AUTHORITY OF SINGAPORE (7 February 2019), <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/FEAT-Principles-Updated-7-Feb-19.pdf>.

cbxxvi Access Now, Human Rights in the Age of Artificial Intelligence, ACCESS NOW (November 2018), <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>.

cbxxvii Monetary Authority of Singapore, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector, 2019, MONETARY AUTHORITY OF SINGAPORE (7 February 2019), <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/FEAT-Principles-Updated-7-Feb-19.pdf>.

cbxxviii Smart Dubai, Artificial Intelligence Principles and Ethics, SMART DUBAI (2019), <https://www.smartdubai.ae/initiatives/ai-ethics>.

cbxxix OECD, The OECD Privacy Framework, OECD (2013), [https://www.oecd.org/digital/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/digital/ieconomy/oecd_privacy_framework.pdf); Robison, S.C., Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI), 63(C) Technology in Society, (2020), <https://ideas.repec.org/a/eee/teins/v63y2020ics0160791x20303766.html>; Christina, H. & Dominik, E, Trust and privacy: How trust affects individuals’ willingness to disclose personal information, IW-Report No 19/2018, (2018) <https://www.econstor.eu/bitstream/10419/179245/1/1023107090.pdf>.

cbxxx The “Transparency and accountability measures” listed in Chapter VI of the upcoming Personal Data Protection Bill, 2019 will create similar obligations for providers.

cbxxxi Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 1 – Accountability, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (August 2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_accountability/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/).

cbxxxii Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principle 1 – Accountability, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (August 2020), [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/principles/p\\_accountability/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/); DSCI, Handbook on Data Protection and Privacy for Developers of Artificial Intelligence (AI) in India: Practical Guidelines for Responsible Development of AI, DSCI (July 2021), <https://www.dsci.in/content/privacy-handbook-for-ai-developers>.

cbxxxiii UK Information Commissioner’s Office, Principle (d): Accuracy, UK INFORMATION COMMISSIONER’S OFFICE, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>.

cbxxxiv Ibid.

cbxxxv IRDAI, Guidelines of Insurance E-commerce, rule 14(a), retrieved from [https://www.irdai.gov.in/admincms/cms/frmGeneral\\_Layout.aspx?page=PageNo3089&flag=1](https://www.irdai.gov.in/admincms/cms/frmGeneral_Layout.aspx?page=PageNo3089&flag=1).

cbxxxvi International Telecommunications Union, GSR 2019 Discussion Paper: Building confidence in a data driven economy by assuring consumer redress, INTERNATIONAL TELECOMMUNICATIONS UNION (2019), [https://www.itu.int/en/ITU-D/Conferences/GSR/2019/Documents/Consumer-Redress-digital-economy\\_GSR19.pdf](https://www.itu.int/en/ITU-D/Conferences/GSR/2019/Documents/Consumer-Redress-digital-economy_GSR19.pdf); UN Conference for Trade and Development, Manual on Consumer Protection, UNCTAD, UNCTAD (2016), <https://unctad.org/en/PublicationsLibrary/webditcclp2016d1.pdf>; Task Force on Financial Redress Agency, Report of the Task Force on Financial Redress Agency, DEPARTMENT OF ECONOMIC AFFAIRS (June 2016), [https://dea.gov.in/sites/default/files/Report\\_TaskForce\\_FRA\\_26122016.pdf](https://dea.gov.in/sites/default/files/Report_TaskForce_FRA_26122016.pdf); Financial Sectors Legislative Reforms Commission, Report of the Financial Sectors Legislative Reforms Commission, DEPARTMENT OF ECONOMIC AFFAIRS (March, 2013), [https://dea.gov.in/sites/default/files/fslrc\\_report\\_vol1\\_1.pdf](https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf); Indian Insitute of Public Administration, Public Grievance Redress and Monitoring System in Government of India Ministries and Departments, DEPARTMENT OF ADMINISTRATIVE REFORMS AND PUBLIC GRIEVANCES (2008), [https://darpg.gov.in/sites/default/files/IIPA\\_Report\\_GRM.pdf](https://darpg.gov.in/sites/default/files/IIPA_Report_GRM.pdf); Kinhal, D., et.al., ODR: The Future of Dispute Resolution in India, VIDHI CENTRE FOR LEGAL POLICY (July 2020), [https://vidhilegalpolicy.in/wp-content/uploads/2020/07/200727\\_ODR-The-future-of-dispute-resolution-in-India.pdf](https://vidhilegalpolicy.in/wp-content/uploads/2020/07/200727_ODR-The-future-of-dispute-resolution-in-India.pdf).

## Acknowledgement

---

On behalf of DSCI, we would like to extend our heartfelt gratitude to all the organizations and individuals for their valuable time and support, without which this guide would not have been possible. This guide is the result of directions and expert inputs of our esteemed advisory group, which included Mr Satyanandan Atyam, Chief Risk Officer of Tata AIF General Insurance Company Limited, and Ms Neelakshi Shalla of Bharati AXA Life Insurance.V

We would also like to thank Omidyar Network India for their support.

## About DSCI

---

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by NASSCOM®, committed towards 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, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives. For more information, visit: [www.dsci.in](http://www.dsci.in)

## Research Partner

---

Dvara Research is a policy research institution based in India. We are a not-for-profit, non-revenue generating policy think tank. Our mission is to ensure that every individual and every enterprise has complete access to financial services. We strongly believe in the deeply transformative power of finance in unlocking the potential of individuals, households, enterprises and local governments.

## Supported By

---

Omidyar Network India invests in bold entrepreneurs who help create a meaningful life for every Indian, especially the hundreds of millions of Indians in low-income and lower- middle-income populations, ranging from the poorest among us to the existing middle class. To drive empowerment and social impact at scale, we work with entrepreneurs in the private, non-profit and public sectors, who are tackling India's hardest and most chronic problems. We make equity investments in early-stage enterprises and provide grants to non-profits in the areas of Digital Identity, Education, Emerging Tech, Financial Inclusion, Governance & Citizen Engagement, and Property Rights. Omidyar Network India is part of The Omidyar Group, a diverse collection of companies, organizations, and initiatives, supported by philanthropists Pam and Pierre Omidyar, founder of eBay.

For more information, visit: [www.omidyarnetwork.in](http://www.omidyarnetwork.in)







## DATA SECURITY COUNCIL OF INDIA

NASSCOM CAMPUS, 4th Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

For any queries, contact:

P: +91-120-4990253 | E: [info@dsci.in](mailto:info@dsci.in) | W: [www.dsci.in](http://www.dsci.in)



[DSCI\\_Connect](#)



[dsci.connect](#)



[dsci.connect](#)



[data-security-council-of-india](#)



[dscivideo](#)

*All Rights Reserved © DSCI 2022*