iab.

India

Cross-Jurisdiction Privacy Project

June 2024

Table of Contents

CJPP India Data Guidance

1. THE DIGITAL PERSONAL DATA PROTECTION ACT (DPDPA)

1.1. Overview & Key Acts, Regulations, and Directives

India's Parliament recently enacted the Digital Personal Data Protection Act, 2023 ("**DPDPA**"). The DPDPA is India's first comprehensive data protection law and will overhaul the existing patchwork of rules on personal data privacy. The purpose and objective of the DPDPA is to provide for the processing of digital personal data in a manner that recognizes both the rights of individuals to protect their personal data and the need to process such personal data for lawful purposes. The DPDPA's provisions are expected to become effective in a phased manner. In pursuance of enabling provisions of the DPDPA, the Central Government will notify implementing rules under the DPDPA.

The DPDPA applies to personal data that is collected in digital form or in non-digital form that is subsequently digitized. "Personal Data" has been defined to mean data about an individual who is identifiable by or in relation to such data.

The DPDPA mandates that any person (e.g., individual, company, firm, association of persons, State) that handles digital personal data must maintain "reasonable security safeguards" to prevent personal data breaches and is liable to pay a penalty for failure to take reasonable security measures, provide notification of personal data breaches, or comply with children's data protection requirements. Notably, the DPDPA does not prescribe or recommend any specific standard that should be implemented to maintain reasonable security safeguards.

DPDPA does not prescribe any criminal penalty or imprisonment.

DPDPA requires companies to obtain consent when collecting or handling personal data and inform the Data Subject ("**Data Subject**") of recipients of such collected data.

It should be noted that DPDPA is broadly consistent with the principles of the GDPR and principles from India's Supreme Court's ("**SC**") ruling in the Privacy Judgment (*defined below*), where the right to privacy was upheld as a fundamental right of an individual under the Indian constitution.

1.2. Guidelines

There are no guidelines applicable to digital advertising in India.

1.3. Background

In *Kharak Singh v. The State of Uttar Pradesh and Others* (1962) the SC held that domiciliary visits by the police at night constitute an unauthorized intrusion into a person's home and a violation of personal liberty. In a majority judgment, the SC ruled that privacy was not a guaranteed constitutional right. Nevertheless, it held that Article 21 of the Constitution was the repository of residuary personal rights and recognized a common law right to privacy.

Furthermore, in *Maneka Gandhi vs. Union of India,* the passport of then-Minister Maneka Gandhi was impounded in "public interest." In this case, the meaning of the word "personal liberty" was again considered by the SC as Maneka Gandhi's passport had been impounded by the Central Government under Section 10(3)(c) of the Passport Act, 1967. Hence, no person can be deprived of such rights, except through procedures established by law. Since the State had not made any law regarding the regulation or prohibition of the rights of a person in such a case, the confiscation of the passport was held to be in violation of Article 21 of the Constitution of India. The SC held that the personal life and liberty of a person must be understood in a broader sense.

In a Writ Petition filed before the SC in 2005, the petitioner stated that mobile telephone service providers and telemarketers violated the law by using the personal data of subscribers for their own business purposes. The SC issued instructions to regulatory authorities to institute measures to reduce such unsolicited calls.

In October 2018, a nine-judge SC bench, in *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors* [Writ Petition (Civil) No. 494 of 2012] ("**Privacy Judgement**") specifically held that the right to privacy is a fundamental right under Article 21 of the Constitution and that it included, at its core, a negative obligation not to violate the right to privacy and a positive right to take all actions necessary to protect the right to privacy.

The SC recognized certain data protection principles such as data minimization, data retention, and data security. This paved way for the legislature to introduce a draft data protection law, namely, The Personal Data Protection Bill (2019) which explicitly addressed data privacy and data protection. The judgement made several observations on the complex relationship between personal privacy and "big data" particularly in the context of how the judicious use of these technologies can result in the State achieving its legitimate interests with greater efficiency. One of the judges in this case identified concerns regarding surveillance and profiling, whereas with respect to private entities, he emphasized the impact of big data and technology on the data intensive generation and its collection and use in a growing digital economy.

The Privacy Judgment changed the contours of Indian privacy law, the interpretation of existing privacy rules, and raised the specter of a robust common law tort of violation of privacy, independent of statutory rules. The SC went on to clarify that any law that encroaches upon the right to privacy is subject to constitutional scrutiny and must meet the three-fold requirement of legality, necessity, and proportionality.

Furthermore, the SC crafted a positive obligation on the government to enact legislation that adequately protects the right to privacy. Various High Courts frequently address data protection issues (e.g., export of data, transfer of data between group companies, and adequacy of consent) from a post-Privacy Judgment perspective. While there is no clear judicial trend yet, it is nevertheless evident that those entities engaging in data collection and processing efforts in India must evaluate and anticipate the impact of the Privacy Judgment on Indian data law.

1.4. Application to Digital Advertising

The DPDPA applies to businesses across all sectors, including digital advertising. The past few years have seen an increase in the introduction of data privacy laws across the Asia-Pacific region, and frequently lawmakers are taking inspiration from the GDPR. The DPDPA follows this trend by incorporating the seven key principles of data protection derived from the GDPR and is expected to trigger a sea change in the way advertisers, publishers, and ad servers collect and process personal data.

Notably, the DPDPA introduces a broad definition of "personal information", creates transparent disclosure requirements for Data Controllers (referred to as "Data Fiduciaries" in the DPDPA) with an emphasis on notice and consent, establishes strong Data Subject rights, provides for the possibility of limitations on cross-border data transfers, and places various obligations on Data Controllers to safeguard personal data. "Data Fiduciaries" is defined as a person who alone or in conjunction with another person determines the purpose and means of processing personal data.

Although inspired by the GDPR in terms of its basic principles, the final version of the DPDPA is far more concise. Some key requirements and restrictions on data processing that have been introduced by the DPDPA, and that may impact digital advertising in India, are listed below:

(a) **Grounds for Processing:** As is the case in many APAC jurisdictions, consent is the primary basis for processing personal data under the DPDPA. The Data Subject's consent is mandatory unless processing is carried out for one of the "legitimate uses" described in the DPDPA. Notably, "legitimate uses" under DPDPA are limited, but they include the processing of information for employment purposes, and where information is voluntarily disclosed by a Data Subject for a specific purpose. They also include processing in response to a medical emergency.

Notably, "legitimate use" under DPDPA is different from "legitimate interest" as the basis of processing under the GDPR. While "legitimate use" is limited to processing only for the limited purposes listed in the DPDPA, "legitimate interest" is more flexible and could in principle apply to any type of processing activity provided that a balancing test demonstrates that such legitimate interest is not overridden by the fundamental rights and freedoms of the data subject. Where consent is the grounds for processing personal data, it must be free, specific, informed, express, and limited to the personal data necessary for fulfilling the specific purposes. This,

in effect, introduces a 'purpose limitation' for the collection of personal data, and suggests that opt-in is the preferred approach. It appears, for example, that all processing of personal data for direct marketing purposes will require prior opt-in consent.

(b) **Consent Notice:** While obtaining consent, a controller must provide Data Subjects with a notice that describes (a) the types of personal data to be processed; (b) the purposes of processing; (c) the method to be used to exercise Data Subject rights and make complaints to the regulator; and (d) contact details of the data protection officer (where required) or a person for individuals to contact to exercise their Data Subject rights. For instance, if the controller wishes to set third-party tracking cookies or pixels that collect Data Subjects' personal data, the controller would need to ensure that the Data Subjects are provided a notice seeking their consent to collect and process their personal data. The requirement to give notice is built into the process of obtaining consent and does not arise where processing is based on "legitimate use".

The DPDPA also requires controllers to translate consent notices into each of India's 22 national languages and empowers the Indian government to impose further requirements under rules for implementation. For instance, a recent Parliamentary Committee Report on the DPDPA suggests that organizations may be required to provide videos and animations to help individuals understand the notice and consent form.

(c) **Data Security and Breach Reporting:** A Data Controller must implement reasonable security safeguards and appropriate technical and organizational measures to ensure compliance with the DPDPA and prevent personal data breaches. Upon the occurrence of a data breach, the law requires a controller to notify the Board and each Data Subject impacted by the incident. The form and manner of such reporting must also comply with the rules that are to be issued by the Indian government. Notably, unlike the GDPR and many data privacy laws in the APAC region, the DPDPA does not create a threshold of risk or harm for breach reporting. This suggests that, at least in theory, it may be necessary to report very large numbers of minor personal data breaches – which has been a problem in the EU under the GDPR even with the inclusion of limited thresholds.

(d) **Data Erasure and Retention Period:** The DPDPA requires Data Controllers to erase personal data when consent is withdrawn or when it is reasonable to assume that the specified purpose is no longer being served. Crucially, the DPDPA also empowers the Indian government to prescribe maximum retention periods for personal data. In other words, the government may prescribe the period within which personal data must be purged in certain circumstances, such as when the Data Subject does not contact the Data Controller for the performance of the specified purpose. The government may set different retention periods for different classes of controllers and for different purposes of processing. This provision will require controllers to formulate their data retention schedules in a manner consistent with the prescribed periods and to ensure that personal data is periodically purged or de-identified.

(e) **Relationship with Processors:** Like the GDPR, the DPDPA recognizes the difference between controllers

(i.e., "Data Fiduciaries" under the DPDPA) – who determine the purposes and means of processing of personal data – and processors, who merely process personal data on their behalf, both in terms of responsibilities and liability for contraventions. It allows controllers to engage third-party processors through written agreements but places the compliance burden solely on controllers. Controllers must, for instance, ensure that processors implement safeguards to protect personal data and erase such data when required to do so under the law. Unlike the GDPR, for example, processors themselves have no obligations or responsibilities under the DPDPA, and, barring the requirement to have a valid contract, no specific conditions are prescribed with respect to sharing personal data between controllers and processors.

Accordingly, advertisers or other entities that act as Data Fiduciaries will need to move swiftly to evaluate their current data processing practices to assess gaps in compliance with the DPDPA, with a view to implementing necessary changes before the relevant requirements take effect. They will need to adopt a flexible approach in the short term, however, taking account of the accompanying rules and guidance that are yet to be published by the Indian government. Below are a few key matters for advertisers or any other players in digital advertising acting as Data Fiduciaries to consider immediately:

(a) Data flows and tracking personal data: Data Controllers should map their personal data flows and understand their current processing activities with respect to Indian personal data.

(b) Consent requirements: Except in limited circumstances where it can rely on a "legitimate use" exception, a Data Controller will need to either obtain opt-in consent from a Data Subject or rely on existing consent to process personal data. Therefore, controllers should immediately examine existing grounds for the processing of personal data and evaluate whether fresh consent from Data Subjects is required once the law takes effect. For instance, where third-party cookies, pixels, or other trackers are deployed to track individuals online; or if personal data is otherwise collected and handled for the purpose of digital advertising, then the entity collecting and handling that personal data would likely have to obtain consent from Data Subjects. Where an entity serves a contextual advertisement without collection of any personal data, it would not require any consent from the Data Subject. However, if personal data is nonetheless collected and processed while serving contextual advertisements, a consent requirement would be triggered. This could include collection of personal data via third-party cookies for purposes such as frequency capping, ad affiliation, click fraud detection, market research, product improvement, debugging, or any other similar purposes.

(c) Revise privacy notices and policies: Data Controllers should consider amending the form and content of privacy policies and consent notices to conform with the DPDPA. Consent notices must include the requisite information and should be translated into local languages.

(d) Breach reporting: The new law requires mandatory reporting of incidents to impacted Data Subjects regardless of their magnitude or risk of harm. This may be a significant departure from the existing policies of

companies, where breach reporting is limited to large-scale incidents. These policies will need to be re-evaluated by Data Controllers and modified.

(e) Children's data: Data Controllers are expressly restricted under the DPDPA from undertaking tracking or behavioral monitoring of children or serving targeted advertisements directed at children. Child is defined as a person under the age of 18. Thus, behavioral advertisements, that rely on third-party trackers to collect information on a child's browsing history, searches, and website activity, i.e., to track or monitor the behavior of a child – would be restricted in India. Entities that are compliant with foreign laws will need to re-examine their practices in India given the difference in the applicable age thresholds.

Of course, many international businesses with operations in India, or that will otherwise be subject to the DPDPA, have already developed sophisticated compliance arrangements designed to address the requirements of the GDPR and/or other data protection laws. These businesses will need to conduct a careful gap analysis to identify the respects in which these arrangements can / need to be rolled out to their Indian operations to facilitate DPDPA compliance. GDPR compliance arrangements may need to be adjusted to take account of the DPDPA's consent-based approach, which is alien to the GDPR compliance culture. For these purposes, compliance approaches developed in the APAC region, where a consent-based approach to data protection is more common, may provide a helpful model. In sum, Data Controllers should evaluate their current practices concerning the data of children to ensure that verifiable parental consent has been obtained for such processing.

2. SCOPE OF APPLICATION

2.1. To whom do the laws/regulations apply, and what types of processing activities are covered/exempted?

The DPDPA applies, with limited exception, to any processing of digital personal data within India.

The term "personal data" is defined broadly and covers any data about an individual that is identifiable by or in relation to such data. Interestingly, the DPDPA does not create sub-categories of personal data, and its provisions apply uniformly, irrespective of the sensitivity of datasets being processed. Statutes in other jurisdictions, such as Singapore and Hong Kong, have taken this approach as well, although regulators have subsequently issued guidance highlighting certain categories of information that is considered sensitive and requiring a higher standard of protection.

"Processing" under the DPDPA is limited to an operation (such as collection, use, storage, transfer, etc.) performed on digital personal data that is wholly or partly automated. Therefore, unlike the GDPR, the DPDPA does not seek to regulate a processing operation or activity that is wholly manual or non-automated.

The DPDPA exempts processing of publicly available personal data, however the exemption is limited to data made publicly available by the Data Subjects themselves or pursuant to pertinent legal requirements. Businesses that rely on public information, such as web crawlers and telemarketing agencies, will therefore not be able to assume that their activities are exempt but will need to carefully consider the scope and application of the DPDPA. This will also be relevant in cases where AI models rely on publicly available information for their processing operations. In these cases, AI-based processing will likely be exempt from the DPDPA, however additional guidance is needed.

Importantly, the exemption under DPDPA is broader than in other jurisdictions. For instance, the GDPR provides a similar exemption, but only limits it to specific restrictions on processing of particularly sensitive personal data; and Singapore law exempts publicly available information only from its consent requirements but not from the law as a whole.

Finally, the DPDPA also excludes from its territorial scope the processing of personal data belonging to offshore individuals when such processing is undertaken in India pursuant to a contract between an India-based entity and an entity located outside India. This exemption likely seeks to benefit Indian outsourcing companies that routinely process data belonging to Data Subjects located outside of India.

2.2. Jurisdictional Reach

Overview

The DPDPA applies to organizations that offer goods or services in India, irrespective of their principal place of business. To the contrary, organizations that collect personal data of individuals overseas and subsequently transfer such personal data to India for processing will not be subject to DPDPA. Their processing activities in India would then likely be covered by data privacy law of the territory wherein data was collected. Thus, contrary to GDPR treatment of extraterritoriality, the DPDPA distinguishes between onshore and offshore processing of personal data.

The transfer of personal data for processing outside India is generally permitted under the DPDPA. However, DPDPA empowers the Indian government to identify specific countries or territories to which data transfers are prohibited. At present, the government has not given any indication of countries that may feature on this list.

Although earlier iterations of the law contemplated allowing transfer only to a specific list of pre-approved territories, the current version of DPDPA provides for the opposite. This contrasts with the strict requirements under GDPR. Some other APAC jurisdictions, including Indonesia and Singapore, have taken a broadly similar, although more flexible, approach than that of the GDPR, requiring entities that transfer personal data overseas to ensure the recipient complies with adequate standards (e.g., by contract). The DPDPA also clarifies that, if its provisions on

international data transfer conflict with other Indian laws, the law which provides a higher degree of protection or restriction on cross-border transfers will prevail. Consequently, sector-specific regulations, such as the Indian central bank's data localization mandate with respect to payment system data, will continue to apply notwithstanding the liberal position contained in the DPDPA.

Application to Digital Advertising

Scenario 1 is the baseline scenario, where the user, publisher, and advertiser are all based in India, where it seems reasonable to assume DPDPA applies.

Scenario 1 (The baseline): A user residing in India (determined by IP address or geo identifier) goes onto an Indian domain and is served an ad by an Indian advertiser. The advertiser uses the user data to build a user profile.

In this scenario, if an Indian domain collects personal data of the user and determines the purpose and means of processing personal data, the Indian domain becomes Data Fiduciary, and the user residing in India becomes Data Subject.

Thus, with respect to a user in India, who visits an Indian domain and is served an ad by an Indian advertiser, any collection, use or disclosure of personal data in connection with this would require consent from the individual, unless one or more of the exceptions to the requirement to obtain consent apply.

The advertiser itself may not be the party collecting personal data. Instead, the party serving the ad and monitoring user interaction, such as the publisher/ad server could be the party collecting personal data and determining the purpose and means of processing. In such a scenario, the party serving the ad would need to obtain consent.

Scenarios 2, 3, and 4 vary depending on the location of the user, publisher, and advertiser to test in each case the jurisdictional reach of the Privacy Laws.

Scenario 2 (User outside India): A Logged-on/signed-in user, known by the publisher to be an Indian resident, goes onto an Indian domain but the user's IP address or geo identifier indicates the user is outside India. An Indian advertiser serves an ad and uses the user data to build a user profile.

If a logged-on/signed-in user, known by the publisher to be a person in India, goes onto an Indian domain but the user's IP address or geo identifier indicates the user is outside India, then DPDPA would still apply when an Indian advertiser serves an ad and uses the user data to build a user profile. This is because personal data is being processed in India by the Indian publisher.

Q1: Does the answer change if this is a signed-out user, with no way of knowing where they are domiciled?

No, the answer would not change. As long as an Indian publisher is collecting and processing personal data which will be processed in India, DPDPA would apply even to signed-out user.

Scenario 3 (Publisher domain outside India): A user residing in India (determined by IP address or geo identifier) goes onto a domain outside of India. An Indian advertiser serves an ad and uses the user data to build a user profile.

A user residing in India would be considered a Data Subject. The applicability of DPDPA to processing activities on the domain would depend on whether the domain typically offers good or services to persons based in India. In such a scenario, collection of Data Subject's personal data would be covered within the extra-territorial applicability of the DPDPA. However, if the domain or advertiser does not supply goods or services to persons based in India, and any collection of personal data of users based in India is only inadvertent, DPDPA would not apply.

Q1: Does the answer change if the site host's content is aimed at Indian residents (e.g. a news aggregator with a section on Indian current affairs)?

No, the answer does not change if the site hosts content aimed at persons in India. To reiterate, as long as the advertiser collects information from a Data Subject located in India, DPDPA applies.

Q2: Does the answer change if the advertiser is based outside of India?

No, the answer does not change. DPDPA would still apply even if the advertiser is based outside India.

Scenario 4 (Advertiser outside India): A user residing in India (determined by IP address or geo identifier) goes onto an Indian domain and is served an ad by an advertiser based outside India. The advertiser uses the user data to build a user profile.

In this scenario, DPDPA will apply to the user residing in India and the entity that collects data at the first instance to build a user profile. Therefore, the provisions of DPDPA will apply to the advertiser based outside India if the advertiser collects data at the first instance and such data is collected from a Data Subject located in India.

Q: Does the answer change if the advertiser has an affiliate/group company based in India?

No, the answer will not change if the advertiser has an affiliate/group company based in India. The user residing in India will be the Data Subject. The advertiser based out of India will be the Data Controller/Data Processor. DPDPA will apply to the entity that collects data at first instance from the Data Subject.

3. DEFINITIONS

3.1. Collect

DPDPA neither defines the term "collect" nor the term "data collector." Correspondingly, the DPDPA refers to the term "Data Fiduciary" instead of "data collector" and lays out certain obligations that a Data Fiduciary must adhere to. For instance, a Data Fiduciary is required to implement reasonable security safeguards and appropriate technical and organizational measures to ensure compliance with DPDPA and prevent personal data breaches.

When a publisher allows an ad tech company's pixel on its page, who is deemed to "collect" personal information and incur legal obligations (e.g., controller/co-controller obligations under GDPR or "business" obligations under CCPA)–the publisher, the ad tech company, or both?

While additional guidance is needed to clarify the answer to this question, a likely outcome, in the ad tech context, is that the publisher is deemed to be "collecting" the personal information and making it available to the ad tech company (even if the publisher does not actually obtain the information itself) given the publisher's determination of the purposes and means of processing along with the ad tech company. Further, it is likely that both the publisher and ad tech company would be considered as joint Data Fiduciaries.

For example, a publisher may integrate an ad tech company's pixel into the publisher's digital property for the purpose of retargeting a visitor to such property. Here, the publisher may be deemed to be determining the purpose (retargeting) and means (use of a pixel to obtain the requisite personal information) of processing and is thus a Data Fiduciary. Further, the ad tech company itself may be deemed a Data Fiduciary, given that the ad tech company may use the data for the purpose of better understanding the visitor generally and will set forth the minimum requisite information that must be collected via the pixel to enable such retargeting (which would speak to the means of processing). In such a case, the publisher and ad tech company would likely be considered joint Data Fiduciaries. There may be exceptions here, such as where the ad tech company is serving purely as the publisher's processor.

Indeed, this analysis would align with case law under the GDPR, where the CJEU has determined that decisions from multiple entities regarding the purposes and means of processing that are "inextricably linked" to each other result in joint controllership.

However, as mentioned, there is no regulatory clarity on this question and we await further guidance.

3.2. Data Processing [i.e., collecting, capturing, retaining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, disclosing, transmitting, dis-

seminating, making available, aligning, combining, restricting, erasing, destroying, or otherwise processing]

DPDPA defines "processing" in relation to personal data to mean *"a wholly or partly automated operation or set of operations on digital personal data, and includes operations such as collection, recording, organization, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination, or otherwise making available, restriction, erasure, or destruction"*.

3.3. Personal Information

Under the DPDPA, "personal data" means *"any data about an individual who is identifiable by or in relation to such data"*. Given this definition, information collected via cookies may be categorized as personal data if it can be used independently, or in combination with other information, to identify a person's identity.

Type of Information Collected	Does this Category Independently Constitute Personal Information? (Yes/No)	Qualifying Notes (if any)
IP Address	No, but see the qualifying note.	–It is not presently clear as to whether tech-nical and persis-tent identifiers, such as IP ad-dress, are personal information under the DPDPA. Further, with respect to other data at-tributes listed in this table, whether or not they are collect-ed in combination with some other data attributes, e.g. pass-port number, that might enable the collector to determine the identity of a given data subject will inform whether the tech-nical persistent identifier can be considered personal data.

Mobile Advertising IDs (IDFA, AAID)	No, but see qualifying note above.	
Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	No, but see qualifying note above.	
Hashed identifiers such as: • Hashed email • Hashed IP address	No, but see qualifying note above.	
User Agent such as: • Character string identifying the application. • Operating system • Browser information, vendor, and/or version of the requesting user agent	No, but see qualifying note above.	
Device Information such as: • Type, version, system settings, etc.	No, but see qualifying note above.	
Website Information such as: • Placement • Title • Creative ID, etc.	No, but see qualifying note above.	
Advertisement Information such as: • Placement • Title • Creative ID, etc.	No, but see qualifying note above.	
Timestamps	No, but see qualifying note above.	

Metrics such as: • Counts • Amounts of time	No, but see qualifying note above.	
Event Data such as: (e.g., full URL including query string, referral URL)	No, but see qualifying note above.	
Precise geolocation (latitude, longitude)	No, but see qualifying note above.	If the individual's specific movements are being tracked, obligations under DPDPA may have to be assessed on a case-to-case basis.
General geolocation (city, state, country)	No, but see qualifying note above.	

- **Are pseudonymous digital identifiers by themselves personal information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)? Please provide context to the above chart.**

The DPDPA's current definition of personal data requires additional guidance. If India takes an approach that is in line with current global practices, then pseudonymous digital identifiers would likely be considered personal data on their own. However, if India adopts an approach that is in line with certain other APAC jurisdictions, then pseudonymous identifiers are only considered personal information if there is additional information available to the business entity that would enable the business entity to link the pseudonymous data with directly identifying data (e.g., actual name).

To clarify, not all data that relates to an individual may identify the individual. For example, a residential address, on its own, relates to a particular house and there could be several individuals residing there.

To the contrary, certain types of data by their nature are likely to identify an individual. This includes data that has been assigned exclusively to an individual for the purposes of identifying the individual (e.g., Aadhaar [Indian national ID] or passport number of an individual); or biometric data (e.g., DNA, facial image, fingerprint). Such unique data would constitute personal data as it can be used to identify an individual.

- **If the answer to the above question is, "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that**

render the pseudonymous information in Database 1 as personal information?

Yes. Persistent digital identifier in Database 1 would likely be considered personal data. This is because when combined with other information in Database 2, the digital identifier can be associated with an identifiable individual.

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "Personal Information"?**

Similar to the use case above, a pseudonymous identifier plus other non-directly identifying data, such as age or gender, may be considered personal information if it can be used in combination to directly identify an individual; however, additional guidance is needed.

- **Is a Company's possession of a pseudonymous identifier "Personal Information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier could be matched to the person, but the Company chooses not to hire such service provider or undertake such transaction. Is the mere fact that this service is potentially available to match to the person sufficient to render that pseudonymous identifier as "Personal Information"?**

No, the mere fact that the Company can potentially hire this service provider who can undertake a transaction to match the pseudonymous identifier to a person, is not sufficient to render that pseudonymous identifier as personal information. Insofar as the Company itself does not possess the means to identify the pseudonymous identifier, it can be reasonably argued that the Company is in possession of non-personal data only.

- **What level of geolocation is Personal Information (precise vs. approximate)? Does it need to be associated with an identifier to be considered Personal Information?**

Geolocation may constitute personal data if a specific individual can be identified from that data, or from that data and other information to which the entity has or is likely to have access. Ultimately, whether such geolocation data constitutes personal data will be dependent on the exact factual scenario at hand. As a starting position, geolocation data, in and of itself, is unlikely to be sufficient to identify individuals. However, once the geolocation data is combined with other information, it may constitute personal data.

Where precise geolocation data of an individual alone (without any other accompanying data) is so distinctive that it could identify an individual, such geolocation alone would constitute personal data.

- **Is a household identifier Personal Information? (Consider: If a company has a residential IP address (household level ID) and multiple unique device IDs (e.g., MAIDs for every mobile device in the house)**

associated with that IP address, would that affect whether the household identifier is considered personal information?)

This would depend on whether specific individuals can be identified with the combination of household-level ID and MAIDs.

If multiple individuals are residing in the same household, household-level ID would constitute personal data only if it is associated with a particular identifiable individual such that the individual can be identified through the data.

- **Is a hashed identifier Personal Information? (Consider: there are commercially available services that will take batches of emails encrypted using standard hashes and return (often a high percentage) of clear emails from them. Does that affect whether they are considered personal information, if all a company has to do is pay for the commercial service?)**

It is unlikely that a hashed identifier would constitute personal data unless the hashing can be reversed and/or there is other information that can be combined to identify the individual.

- **Is probabilistic information considered Personal Information?**

As discussed iin responses above, if the information in question can identify any individual, whether on its own or together with other information that an entity has access to, then it would likely constitute personal data.

3.4. Sensitive Data

DPDPA does not create subcategories of personal data, such as sensitive data. Its provisions apply uniformly irrespective of the sensitivity of datasets being processed. Statutes in other jurisdictions, such as Singapore and Hong Kong, have taken this approach, although regulators have subsequently implemented guidance notes and codes of practice highlighting certain categories of information that may be considered sensitive and stating that, where appropriate, personal data of a sensitive nature should be subject to a higher standard of protection.

3.5. Pseudonymous Information

- **Is pseudonymous information considered Personal Information?**

DPDPA does not define pseudonymous information. If digital identifiers can establish the identity of a Data Sub-

ject, they will be considered Personal Data. That said, data which has been irreversibly anonymized would not constitute personal data.

- **Are persistent digital identifiers pseudonymous information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)?**

Persistent identifiers by themselves would not be categorized as Personal Information but may be categorized as Personal Information if they can be used independently or in combination with other information to identify a person's identity.

- **Does the law subject pseudonymous information to fewer obligations than "regular" personal information?**

Generally, standalone pseudonymous information would not constitute personal data. If, however, pseudonymous information can be easily re-identified to establish the identity of individuals, then such pseudonymous information would likely trigger obligations under DPDPA.

3.6. Anonymized/de-identified Information

DPDPA does not contain provisions that define anonymized/de-identified information.

- **Is there a difference between anonymized or de-identified data?**

There is neither any definition of anonymization/de-identified data provided under DPDPA, nor does the DPDPA prescribe any specific procedure or standards of the irreversibility of anonymized/de-identified data. DPDPA also does not explicitly prohibit re-identification and processing of re-identified data. In absence of specific provisions under DPDPA, it appears that de-identification of data would likely be treated on par with deletion. This implies that once data is de-identified or anonymized, it would no longer come with the ambit of DPDPA.

- **What common data categories are passed between publishers, advertisers, and ad tech companies that fall into this category when no persistent identifier is present (e.g., browser type, device type, operating system, app name, publisher site)?**

Based on publicly available information, some commonly passed data categories include:

(a) Search history;
(b) Time of session;
(c) Purchase/interaction behavior;

(d) Demographics; and
(e) Interaction with advertisement.

3.7. Data Controller and Processor

3.7.1. Data Controller

As discussed earlier, DPDPA does not define the term "Data Collector." Correspondingly, the DPDPA refers to the term "Data Fiduciary" instead of "Data Collector." The term "Data Fiduciary" has been defined as follows:

"any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data."

3.7.2. Joint Controller/Co-Controller

DPDPA does not define "joint controller" or "co-controller." In India, any entity, that alone or in conjunction with another entity determines the purpose and means of processing personal data, is treated as a data fiduciary (akin to a controller) and must severally comply with the obligations of a data fiduciary. Unlike the GDPR, joint-controllers or co-controllers are not jointly liable under the law and cannot claim that loss caused to a Data Subject is not attributable to their processing activities but is attributable to the processing by their joint controller.

In the digital advertising context, website operators routinely embed advertiser plugins on their website, enabling visitors to engage with advertiser content with a simple click. When website operators embed third-party advertising plugins, the advertiser's content is displayed on the website. These plugins transmit visitor's personal data to the advertiser. In this scenario, when visitors access the website, their personal data is transmitted to the advertiser via the plugin, regardless of whether they interact with the content or whether they are users of the advertiser's platform. Both the website operator and advertiser would likely qualify as Data Fiduciaries or co-fiduciaries under DPDPA to the extent they determine (albeit independently) the purpose and means of processing personal data. In the event of any harm or loss to the Data Subject owing to data breach, the entire liability will be undertaken by both parties severally. This is different from their treatment under GDPR. Under the GDPR, website operators embedding third-party advertising plugins (i.e., the website operator) can be considered joint controllers with the advertiser. However, the website operator's liability will only be limited to the extent to which they determine the purposes and means of processing personal data (i.e., collection and transmission).

3.7.3. Data Processor/Service Provider (i.e., an entity that is qualified as a pro cessor or service provider under the law because it meets certain requirements and processes data pursuant to a permissible purpose on behalf of a control ler/business)

"Data Processor" means any person who processes personal data on behalf of Data Fiduciary.
Like the GDPR, DPDPA recognizes the difference between Data Fiduciaries – who determine the purpose and means of processing personal data – and processors, who merely process personal data on their behalf, both in terms of responsibilities and liability for contraventions. It allows controllers (or Fiduciaries) to engage third-party processors through written agreements but places the compliance burden solely on Data Fiduciaries. Data Fiduciaries must, for instance, ensure that processors implement safeguards to protect personal data and erase such data when required to do so under the law. Unlike under the GDPR, for example, processors themselves have no obligations or responsibilities under the DPDPA, and, barring the requirement to have a valid contract, no specific conditions are prescribed with respect to the sharing of personal data between controllers and processors.

3.7.4. Third Party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements un der the law as to such data, such as a third-party under the CCPA)

DPDPA does not define "Third Party."

4. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

4.1. Overview

DPDPA puts in place the following key obligations on Fiduciaries with respect to their data collection and processing activities:

(a) ***Notice and Consent Obligation:*** The entity must obtain an individual's consent before collecting, using, or disclosing his/her personal data for a purpose. While obtaining consent, the entity must provide Data Subjects with a notice that describes (a) the types of personal data processed; (b) the purposes of processing; (c) the method to be used to exercise Data Subject rights and make complaints to the regulator; and (d) contact details of the data protection officer (where required) or a contact person for individuals to contact to exercise their Data Subject

rights.

(b) ***Purpose Limitation Obligation:*** The entity may only collect or process personal data only for a lawful purpose for which the Data Subject has given their consent; or for certain legitimate uses.

(c) ***Accuracy Obligation:*** The entity must ensure completeness, accuracy, consistency of personal data, if it is likely to be used to make a decision that affects Data Subject; or disclosed to another Data Fiduciary.

(d) ***Security Obligation:*** The entity must implement appropriate technical and organizational measures to ensure effective observance of provisions of DPDPA.

(e) ***Retention Limitation Obligation:*** Unless retention is necessary to comply with law, the entity must erase personal data upon Data Subject withdrawing their consent; or as soon as it is reasonable to assume that specified purpose is no longer served; whichever is earlier.

(f) ***Grievance Redressal Obligation:*** In the event of personal data breach, the entity must give intimation of such breach to the Data Protection Board and each affected Data Subject.

4.2. Accountability

4.2.1. Overview

Data Fiduciaries are responsible for complying with the provisions of DPDPA in respect of any processing undertaken by them or on its behalf by Data Processor. Every Data Fiduciary must also publish the contact information of a data protection officer, of any person who is able to answer on behalf of Data Fiduciary, questions raised by data Subjects about processing of their personal data.

4.2.2. Application to Digital Advertising

The Accountability Obligation (discussed in Section 4.2.1 above) is of general application and applies to all entities, including entities that engage in digital advertising activities in India, in the capacity of Data Fiduciaries.

4.3. Notice

4.3.1. Overview

While obtaining consent, a Data Fiduciary must provide Data Subjects with a notice that describes (a) the types

of personal data processed; (b) the purposes of processing; (c) the method to be used to exercise Data Subject rights and make complaints to the regulator; and (d) contact details of the data protection officer (where required) or a contact person for individuals to contact to exercise their Data Subject rights.

The requirement to give notice is built into the process of obtaining consent and does not arise where processing is based on "legitimate use". The DPDPA requires Data Fiduciary to translate consent notices into each of India's 22 national languages and empowers the Indian government to impose further requirements under rules for implementation. For instance, a recent Parliamentary Committee Report on the DPDPA suggests that entity may be required to provide videos and animations to help individuals understand the notice and consent form.

Who must receive notice?

Data Subjects, whose personal data will be collected, used, or disclosed must be notified of the purposes of such collection, use, or disclosure. The notification would generally have to take place before or at the time of collection of such data.

- **Are there any requirements compelling vendors directly collecting Personal Information or those receiving it from others Personal Information to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

As per DPDPA, the entity that determines the purpose and means of processing personal data is responsible for providing notice to Data Subjects. While additional guidance is needed, if a vendor jointly controls the purposes and means of collection, then a contract would likely be necessary that stipulates that the Data Fiduciary that is end-user-facing will place proper notice in front of that data subject.

- **Who must receive notice? When must notice be provided? What must be in the notice in the digital advertising context? (Consider also, what notice needs to be provided when pixels fire on a webpage?)**

Please refer to our response above.

- **Is there specific notice required for sensitive information?**

No. DPDPA does not distinguish sensitive personal data from any other type of personal data.

- **Are there any specific requirements for providing notice related to processing children's Personal Information?**

While there is no specific requirement under DPDPA for providing notice related to processing of children's data, it

is important to note that Data Fiduciary can only process a child's (i.e., any individual below 18 years of age) data after obtaining verifiable consent of a parent or a guardian. Moreover, any tracking and behavioral monitoring of children or targeted advertising towards children is prohibited. Notably, this restriction applies to all Data Fiduciaries and is not specifically applicable to Data Fiduciaries that focus on processing children's data or are otherwise aware that they are collecting and processing children's data.

Notably, the government may exempt certain Data Fiduciaries from these additional obligations based on the type of processing or Fiduciary involved. However, in order to rely on this exemption, a Fiduciary would need to demonstrate to the government that its processing is verifiably safe.

- **Are there any requirements compelling vendors directly collecting personal Information or those receiving it from others personal information to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

Please refer to our response on page 20 to the question concerning collection of personal information by vendors.

4.3.2. Application to Digital Advertising

- **Do third parties need to be named? For example, if a publisher gives privacy policy notice that it may share personal information with third parties for advertising purposes, does it have to specify which third parties? Do specific digital advertising activities or purposes need to be disclosed as well (e.g., TCF purposes)?**

No, there is no specific requirement in DPDPA for third parties to be named in a privacy notice or policy. While the DPDPA requires purposes to be disclosed, it does not specify the level of detail required. Entities that opt to disclose TCF purposes may do so as there is no specific guidance on the granularity of purposes to be specified in the notice seeking consent. However, the forthcoming rules to be notified under the DPDPA would likely provide clarity on this aspect.

- **From an industry perspective, it is common to distinguish data use for ad targeting vs. profile building vs. measuring ad campaigns. Does the notice requirement require separate disclosure of those things, or is it enough to say something general like, "advertising and related purposes"?**

Notification is required for all uses of personal data, i.e., for ad targeting, profile building, and measuring ad campaigns.

4.4. Consent and Exceptions to Consent

4.4.1. Overview

As in many jurisdictions in the APAC region, consent is the primary ground for processing personal data under the DPDPA. Consent of a Data Subject is mandatory unless processing is carried out for one of the "legitimate uses" described in the DPDPA (discussed below). Such consent must be free, specific, informed, express, and limited to the personal data necessary for fulfilling the specific purposes. This, in effect, introduces a 'purpose limitation' for the collection of personal data, and suggests that opt-in is the preferred approach.

- **For what types of Personal Information or purposes of processing is consent required?**

Consent is required for any type of digital personal data, subject to the exceptions stated above.

- **How is valid consent manifested–express consent, opt-in, implied consent, or opt-out?**

Consent must be unconditional and unambiguous with clear and affirmative action. This implies that a valid consent would typically require a positive opt-in. It is not advisable to use pre-ticked boxes or any other method of default consent.

- **Is specific notice required as part of the consent?**

Yes, prior to obtaining consent from an individual, an entity must notify the individual of the purposes for which his personal data will be collected, used, or disclosed. If the entity fails to inform the individual of the purposes for which his/her personal data will be collected, used, and disclosed, any consent given by the individual would likely not amount to valid consent under DPDPA.

- **Does the consent obligation require granularity (i.e., consent for distinct processing activities) similar to GDPR? Or is the consent obligation more generalized (e.g., requiring consumers to opt-in to "online behavioral advertising" more broadly, without having to consent to each constituent processing activity/party)? Is consent different for different uses or types of data (e.g., sensitive data, profiling, automated decision making, etc.) Please provide details.**

The DPDPA does not specify the level of detail to which consent must be obtained. The general principle is that consent should be informed and should be for the specified purpose, among other things. Thus, an individual only gives valid consent if the individual has been notified of the purposes for which his/her personal data will be collected, used, or disclosed and the individual has provided consent for those purposes.

Generally, the entity should state its purposes at an appropriate level of detail for the individual to determine the reasons and manner in which the entity will be collecting, using, or disclosing personal data.

- **Can Personal Information be processed for secondary purposes (i.e., differing purposes from which it was collected)?**

No, personal information cannot be processed for secondary purposes unless consent has been obtained for that purpose.

- **Are there any rules compelling downstream recipients/processors of personal information to provide additional notices?**

There are no provisions under DPDPA compelling downstream recipients/processors of Personal Information to provide additional notices.

- **Are there any issues concerning the timing of consent?**

An entity must obtain the consent of the individual before or at the time of collecting personal data for a purpose. If the purpose for which the personal data will be used was not notified to the individual before the collection of personal data, the individual must be informed of this purpose, before handling of the personal data for that purpose and must provide his consent for such handling, as the case may be.

- **Are there distinct consent requirements for sensitive Personal Information?**

There are no distinct consent requirements for sensitive personal information.

- **Are there distinct consent requirements for profiling consumers? If a business gets consent to use personal data for "advertising and marketing" purposes, is a separate (or more specific) consent required to build an advertising profile for advertising?**

There are no distinct consent requirements for profiling consumers.

- **Are there distinct consent requirements for automated decision making?**

There are no distinct consent requirements for automated decision-making.

- **Are there any age restrictions related to consent? Are there distinct consent requirements around processing children's Personal Information?**

Yes, there are distinct requirements for processing children's personal information. Please refer to our response to the question concerning children's data above for a detailed explanation.

- **Can consent, however manifested, be revoked?**

Yes, consent can be revoked by Data Subject. Once consent is revoked, Data Fiduciary must cease processing activities on such personal data.

4.4.2. Application to Digital Advertising

There are no specific consent requirements for digital advertising; however, consent is required where there are digital marketing activities that involve the collection, use, and disclosure of personal data.

4.5. Appropriate Purposes

4.5.1. Application to Digital Advertising

- **Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).**

DPDPA does not require a specific legal basis for specific digital advertising activities. Also, DPDPA does not define "profiling" and does not mirror privacy provisions of the GDPR or California Consumer Privacy Act, 2018.

- **If yes, what are the legal bases (e.g., consent, legitimate interest)? Are there any requirements related to lawful basis (need a valid legal basis to process) fairness (scope of processing is fair) transparency (transparent about the processing activity to the consumer and the lawful basis)?**

As in many jurisdictions in the APAC region, consent is the primary ground for processing personal data under the DPDPA. Consent of a Data Subject is mandatory unless processing is carried out for one of the "legitimate uses" described in the DPDPA (discussed below), however digital advertising is not presently one of the enumerated legitimate uses. Such consent must be free, specific, informed, express, and limited to the personal data necessary for fulfilling the specific purposes. This, in effect, introduces a 'purpose limitation' for the collection of personal data, and suggests that opt-in is the preferred approach.

The DPDPA does permit processing without consent for certain legitimate uses. These are limited, but they include the processing of information for employment purposes, and where information is voluntarily disclosed by a Data Subject for a specific purpose. They also include processing in response to a medical emergency. Although these will be helpful to bridge the gap between the consent requirement and the wide range of processing operations which should reasonably be expected to go ahead irrespective of consent, the pre-GDPR European experience suggests that the absence of a relatively broad "legitimate interests" concept to justify processing without consent is likely to prove problematic for Indian businesses building DPDPA compliance programs. It appears, for example, that all processing of personal data for direct marketing purposes will require prior opt-in consent, even in a B2B context.

- **Does the law address processing for secondary purposes/differing purposes from which it was collected?**

Yes. Personal information collected from Data Subjects must only be used for the purposes for which it was collected. Accordingly, such information cannot be used for secondary/differing purposes. Safeguards

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

Under the DPDPA, Data Subjects have the following key rights:

- **A right to access information regarding the personal data being processed.**
- **A right to withdraw consent.**
- **A right to correct, erase or update personal data.**
- **A right to redress for grievances.**
- **A right to appoint a nominee to exercise rights in case of death or incapacity.**

Data Fiduciaries will need to revisit existing mechanisms (if any) to deal with Data Subject Access Requests. Fiduciaries will also have to be more proactive and transparent in dealing with grievances or complaints with respect to their data processing activities.

5.2. Access

Data Subjects have the right to access their personal data.

5.3. Rectify

Data Subjects have the right to review and correct their personal data.

5.4. Deletion/Erasure

Data Subjects have the right to request deletion of their personal data.

5.5. Restriction on Processing

There is no separate right to restrict processing of personal data under the DPDPA, so long as the consent obligation is adhered to, including that the individual's valid consent is given for that purpose.

5.6. Data Portability

This right is provided under DPDPA.

5.7. Right to Object

This right is currently not provided to Data Subjects under DPDPA.

5.8. Right Against Automated Decision-making

This right is currently not provided to Data Subjects under DPDPA.

5.9. Responding to Consumer Rights Requests

In case a Data Subject makes any request regarding his/her Personal Information, please refer to our response in Paragraph 9.1 below.

5.10. Record Keeping Concerning Rights Requests

DPDPA does not expressly impose any overarching record-keeping requirements concerning requests by Data Subjects.

5.11. Is providing consumers with these rights required by law or mere suggestions?

Providing consumers with these rights is required by law.

5.12. Application to Digital Advertising

With respect to digital advertising, a consumer's data subject rights typically flow from the moment a publisher collects or processes their Personal Information. In the event that a publisher or ad tech company utilizes a consumer's Personal Information, the consumer will have the right to request that the publisher or the ad tech company to stop using his/her Personal Information. In such instances, apart from the publisher/ad tech company refraining from using the Personal Information, the publisher/ad tech company must also intimate the concerned service provider to stop using such data, to the extent possible.

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

Like the GDPR, the DPDPA recognizes a difference between Data Fiduciaries (controllers) that determine the purpose and means of processing, and processors that only process personal data on their behalf, both in terms of responsibilities and liability for wrongdoing. The DPDPA allows controllers to engage third-party processors through written agreements but places the compliance burden solely on the controller. Controllers must, for instance, ensure that processors implement safeguards to protect personal data and erase such data when required to do so under the law. Unlike the GDPR, for example, processors themselves have no obligations or responsibilities under the DPDPA, and barring the requirement to have a valid contract, no specific conditions are prescribed with respect to the sharing of personal data between controllers and processors.

6.2. Data Controller Outsourcing of Processing

The DPDPA does not establish any framework for outsourcing of processing activities by Data Fiduciary. As mentioned earlier, DPDPA places the ultimate responsibility on Data Fiduciary, not Processor, for compliance with privacy obligations.

6.3. Data Processor Rights and Responsibilities

The DPDPA does not establish any framework for outsourcing of processing activities by Data Fiduciary.

6.4. Application to Digital Advertising

The provisions applicable to Data Fiduciaries as mentioned above would apply to entities in all instances of digital advertising as well.

7. DATA TRANSFER & OUTSOURCING

7.1. Overview

The transfer of personal data for processing outside India is generally permitted under the DPDPA. However, the law empowers the Indian government to identify specific countries or territories to which data transfers are prohibited. At present, the government has not given any indication of the countries that may appear on this list.

Although earlier iterations of the law contemplated a 'whitelist' approach that allows transferring personal data only to a specific list of pre-approved territories, the government has yielded to industry pressure and the current version of the DPDPA provides a more favourable 'blacklist' approach. This, of course, contrasts with the strict requirements under the GDPR. Some other APAC jurisdictions, including Indonesia and Singapore, have taken a broadly similar, although more flexible, approach than that of the GDPR, imposing a requirement on entity transferring personal data overseas to ensure the recipient complies with adequate standards (for example, that it is subject to legally binding obligations that contain the same or a higher level of protection as is afforded under the local law).

The DPDPA also clarifies that if its provisions on international data transfer conflict with other Indian laws, the law which provides a higher degree of protection or restriction on cross-border transfers will prevail. Consequently, sector-specific regulations such as the RBI's data localization mandate concerning payment system data, will continue to apply notwithstanding the liberal position contained in the DPDPA.

7.2. Application to Digital Advertising

If the Data Fiduciary in digital advertising intends to transfer Personal Information collected, the entity is required to comply with transfer restrictions detailed above.

8. AUDIT/ACCOUNTABILITY

8.1. Overview

- **Audit - What audit rights are dictated by law (e.g., must companies have audit rights over their vendors? Does it matter what the classification of those vendors are?)**

The DPDPA empowers the Indian government to identify a Data Controller or a class of Data Controllers as "Significant Data Fiduciaries" based on factors such as the volume and sensitivity of data being processed, and the level of risk presented to the rights of Data Subjects. This concept is broadly equivalent to the various tests in the GDPR for the application of some of its "accountability" requirements, but with a greater degree of discretion in the hands of government.

Significant Data Fiduciaries have specific obligations over and above those applicable to general Data Controllers. These include appointing a Data Protection Officer based in India, appointing an independent data auditor, and conducting periodic Data Protection Impact Assessments (DPIAs) and data audits.

- **Accountability - Must companies/vendors keep certain records to prove they have met certain requirements? What are those requirements?**

For entities that have delegated work to vendors, the entity itself remains liable to comply with the DPPDA for the personal data collected and processed. However, to date, there are no mandatory audit rights under law for companies over their vendors. Instead, the audit rights over vendors must be clearly specified within the agreements between the companies and vendors.

8.2. Application to Digital Advertising

There is no provision specific to digital advertising for audit and record-keeping purposes.

9. DATA RETENTION

9.1. Overview

DPDPA requires entities to dispose of personal data or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which the personal data was collected is no longer necessary for legal or business purposes.

10. DATA PROTECTION AUTHORITY

10.1. Overview

(a) ***The Data Protection Board of India ("Board"):*** The Board will be established by the Central Govern ment for the purpose of processing complaints and conducting hearings. Civil courts are prohibited from intervening in matters under the Board's purview.

(b) ***Independence and Qualifications of the Board:*** The Board, labeled as an 'independent body', has its composition and terms determined by the Central Government, raising concerns about its true independence. Qualifications for Board members are not explicitly outlined, though it may include representation from judicial and technical backgrounds.

(c) ***Proceedings Before the Board:***

(i) ***Power to Inquire:*** The Board can initiate inquiries based on intimation, complaints from Data Subjects, or references by the Central Government, following principles of natural justice.

(ii) ***Powers of the Board During Proceedings:*** Endowed with civil court powers, the Board can summon evidence but cannot impede daily operations.

(iii) ***Orders Passed by the Board:*** The Board may issue interim or final orders, including penalties for data breaches. It can also take corrective actions and impose costs for false or frivolous complaints.

(d) ***Appeals to TDSAT (Telecom Disputes Settlement and Appellate Tribunal):*** TDSAT will serve as the Appellate Tribunal. Appeals must be made within 60 days, and the TDSAT will operate digitally, aiming for expeditious resolutions. TDSAT's orders will be considered civil court decrees, with appeals to the Supreme Court required within 90 days.

10.2. Main Regulator for Data Protection

The Ministry of Electronics and Information Technology ("MeitY") operates as the nodal agency for information technology in India.

10.3. Main Powers, Duties and Responsibilities

MeitY's role has been restricted to the formulation of policy. Application to Digital Advertising

11. SANCTIONS

11.1. Liability

- **Scope of liability for publishers and advertisers for processing activities of ad tech companies**

Non-compliance with the DPDPA may lead to the imposition of significant penalties. A data fiduciary's failure to take reasonable security measures may lead to a penalty of up to INR 250 crores (approximately USD 30 million), whereas failure to notify of a personal data breach or comply with children's data protection requirements may lead to penalties of up to INR 200 crores (approximately USD 24 million). Penalties for any other non-compliance may range from INR 50 crores (approximately USD 6 million) to INR 150 crores (approximately USD 18 million). The procedure for imposition of these penalties is to be separately prescribed.

- **Scope of liability for ad tech companies for collection activities of publishers and advertisers**

Please refer to response above.

11.2. Enforcement and Market Practice

- **How are claims raised under the law?**

Claims are usually raised by providing notice. In the event the Data Collector or processor does not address the Data Subject's concerns, the Data Subject has the option of filing a complaint with the Board.

- **Who enforces them?**

The Board.

- **What is their practice (quietly working with companies to fix, publicly coming out with large investigations? Fact specific?)**

We do not have sufficient information in this regard.

- **What guidance has there been to date showing how to handle requirements in the ad ecosystem? Have the regulators been educated on how the ecosystem operates? Have compliance regimes been discussed with them? Has their feedback been solicited?**

We do not have sufficient information in this regard.

11.3. Private Right of Action

DPDPA allows Data Subjects whose data privacy rights have been violated to seek recourse for disputes arising out of violation of privacy. Data Subjects have the right to avail grievance redressal mechanism offered by Data Fiduciaries. Further, Data Subjects can make complaints to the Board in the event of personal data breach or non-compliance by Data Fiduciary.

11.4. Digital Advertising Liability Issues

N/A

12. NOTIFICATION | CERTIFICATION | REGISTRATION

12.1. Requirements and Brief Description

DPDPA does not require Data Collectors or Data Processors to be registered in India.

12.2. Application to Digital Advertising

N/A

13. DATA PROTECTION OFFICER

13.1. DPO – Compulsory Appointment (Yes/No)

Yes, a Data Fiduciary must appoint a Grievance Officer.

13.2. Requirements

The Data Fiduciary must publish the name and contact details of the grievance Officer on its website. As good practice, entities should appoint a grievance officer who is located in India.

13.3. Application to Digital Advertising

N/A

14. SELF-REGULATION

14.1. Overview

- **Are there any industry-self regulatory schemes in place in the jurisdiction?**

There is no central regulatory agency or overarching legislation regulating the advertising industry or, more specifically, digital advertising in India. Notably, the Indian advertising market is regulated by a non-statutory body called the Advertising Standards Council of India ("**ASCI**"). The ASCI has adopted a Code for Self-Regulation in Advertising ("**ASCI Code**"), which applies to all persons involved in the commissioning, creation, placement, or publishing of advertisements. The ASCI Code primarily discusses the content and form of advertising and has been drawn up with a view to achieving the acceptance of fair advertising practices in the best interest of the consumers.