INDUSLAW
THOUGHT LEADERSHIP ... APPLIED

DATA PROTECTION FRAMEWORK FOR INDIA

FOREWORD

> *Informational privacy is a facet of the right to privacy.*
>
> Justice K.S. Puttaswamy (Retd.) v. Union of India

The white paper released by the Ministry of Electronics and Information Technology (MeitY) on the proposed 'data protection regulatory framework for India' in November 2017, has discussed various aspects of data protection and analysed pertinent issues from the standpoint of laws in several jurisdictions. The white paper also provides provisional views which we believe could be the foundation for the proposed data protection legislation. Some of key issues that find a prominent place in the white paper are the territorial jurisdiction under the proposed law, nature of personal data and sensitive personal data protected and the rights associated therewith, cross border flow of data and authorities responsible for controlling and processing data. Overall, the white paper suggests that the proposed data protection legislation should not only provide a means to protect personal information but also put in place processes to regulate the mechanism for receiving, storing and processing data and provide remedies in instances of data breach. It is our belief that the legislative process adopted for the proposed data protection legislation, which includes seeking inputs from stakeholders, academicians, lawyers etc., will ensure that the data protection regime in India is more robust, has a holistic view and adopts international best practices in relation to data protection.

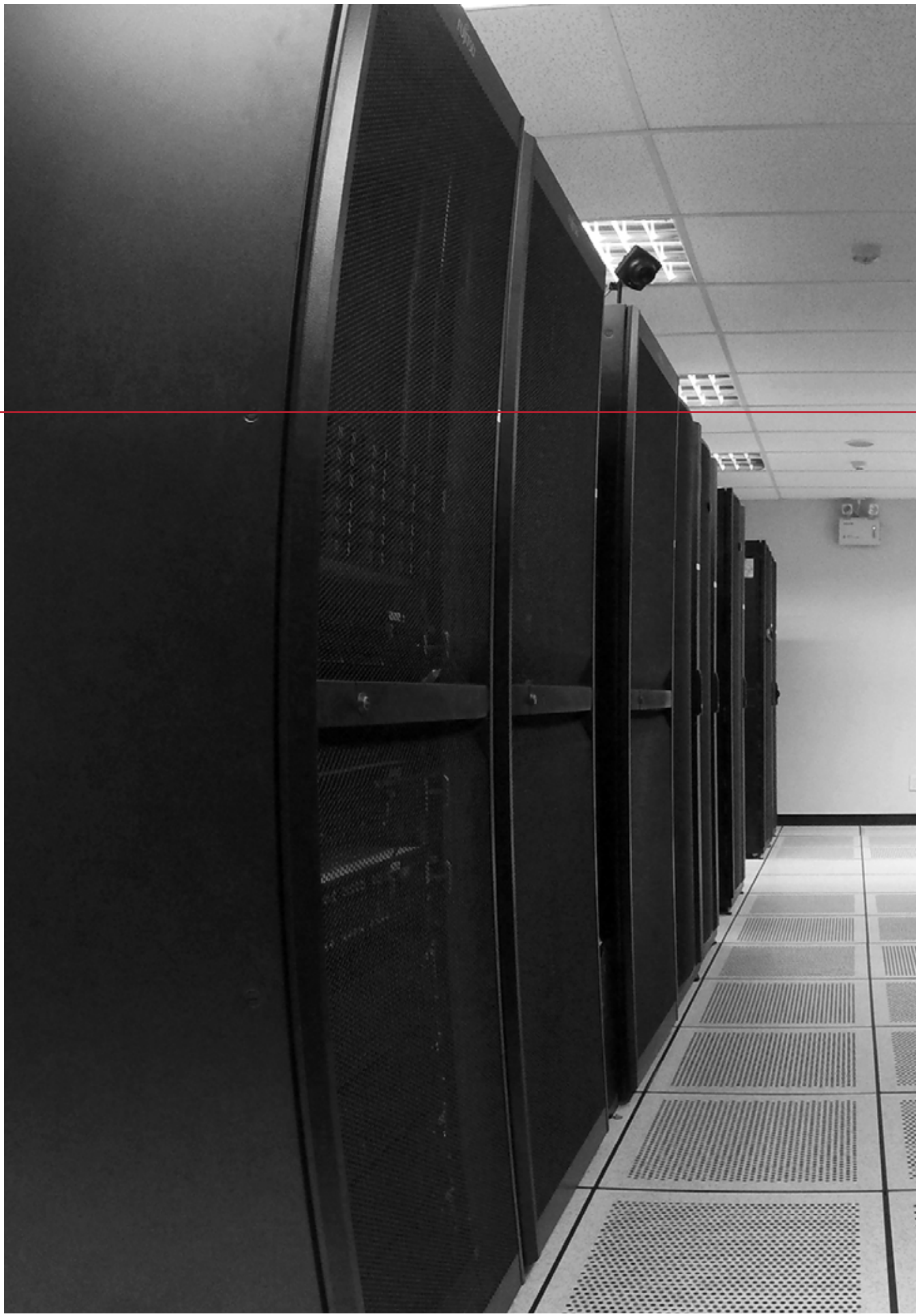
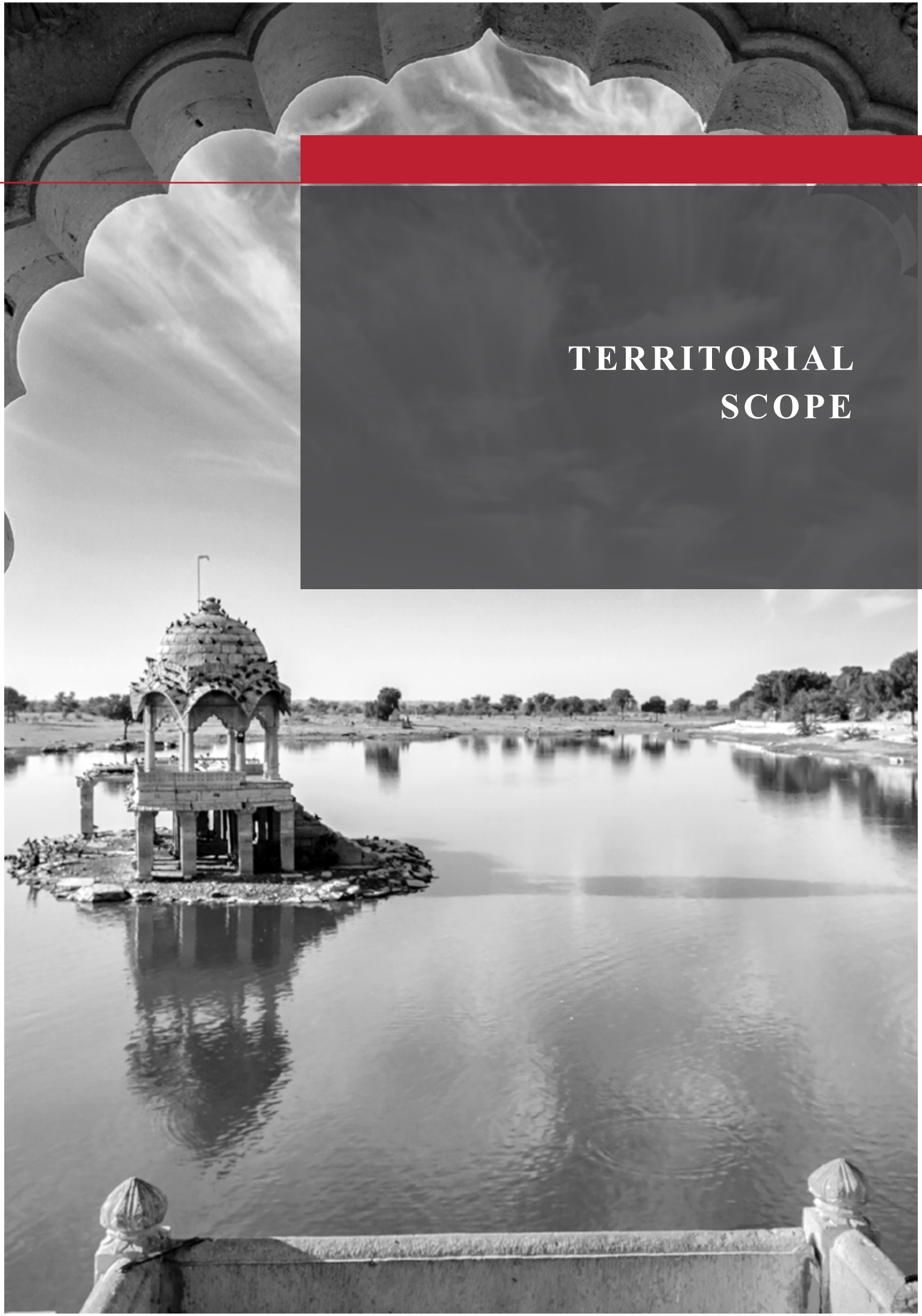


TABLE OF CONTENTS



TERRITORIAL SCOPE

Proposed DP Law should have extra-territorial application, making offences punishable against entities collecting personal data from Indian residents, irrespective of their presence in India. To ensure enforceability of the law, certain minimum, non-negotiable terms that parties must include in their contracts should be laid down in the Proposed DP law.

Civil Matters

Indian courts have jurisdiction over civil matters in which the wrong is committed in India or the place of residence, employment or carrying on of business is located within India. The proposed data protection legislation (**"Proposed DP Law"**) should clarify the basis of jurisdiction on the grounds of *'carrying on business in India'*, perhaps by way of an explanation under the relevant section, such that persons who do business transactions with persons located in India may be brought under Indian jurisdiction.

Extraterritorial Application of Indian Criminal Law

Extraterritorial application of Indian criminal law is provided on the basis that an offence was committed by an Indian citizen anywhere in the world or any offence committed on board a ship or airplane registered in India. Further, any offence that is targeted, by any person from any location, against a computer, computer system, computer network or computer resource located in India would confer jurisdiction upon Indian courts.

The effect of the offence being felt in India or a threat to Indian security or the security of its citizens, and not presence of the offender in India, is the key to establishing jurisdiction.

The Proposed DP Law in India should have extra-territorial application, making punishable offences against personal data of Indian residents by entities offering goods or services to them, regardless of the location of the data processor or their presence in India. In this context, it would be necessary to ensure that the governing law and jurisdiction in the contract *(including terms of use and privacy policy)* between the individual and such foreign entity should be India. Alternatively, the governing law and jurisdiction should not restrict the individual's right to take action under the Proposed DP Law. The benefit will be two-fold - protection of individual rights and payment of compensation by such entities for any violation of such laws. Additionally, compensation payable to an individual should include not only wrongful loss or wrongful gain *(i.e. objective harm)* but also subjective harm so that anticipated loss owing from collection of personal information is also covered. The test to determine jurisdiction can be any of the following factors - (i) processing of personal data of Indian data subjects similar to the European Union's GDPR, whether or not such processing happens in India; (ii) the entity performing the processing undertakes business or derives revenues or profits from Indian data subjects; or (iii) the processing of personal data of any person takes places in India.

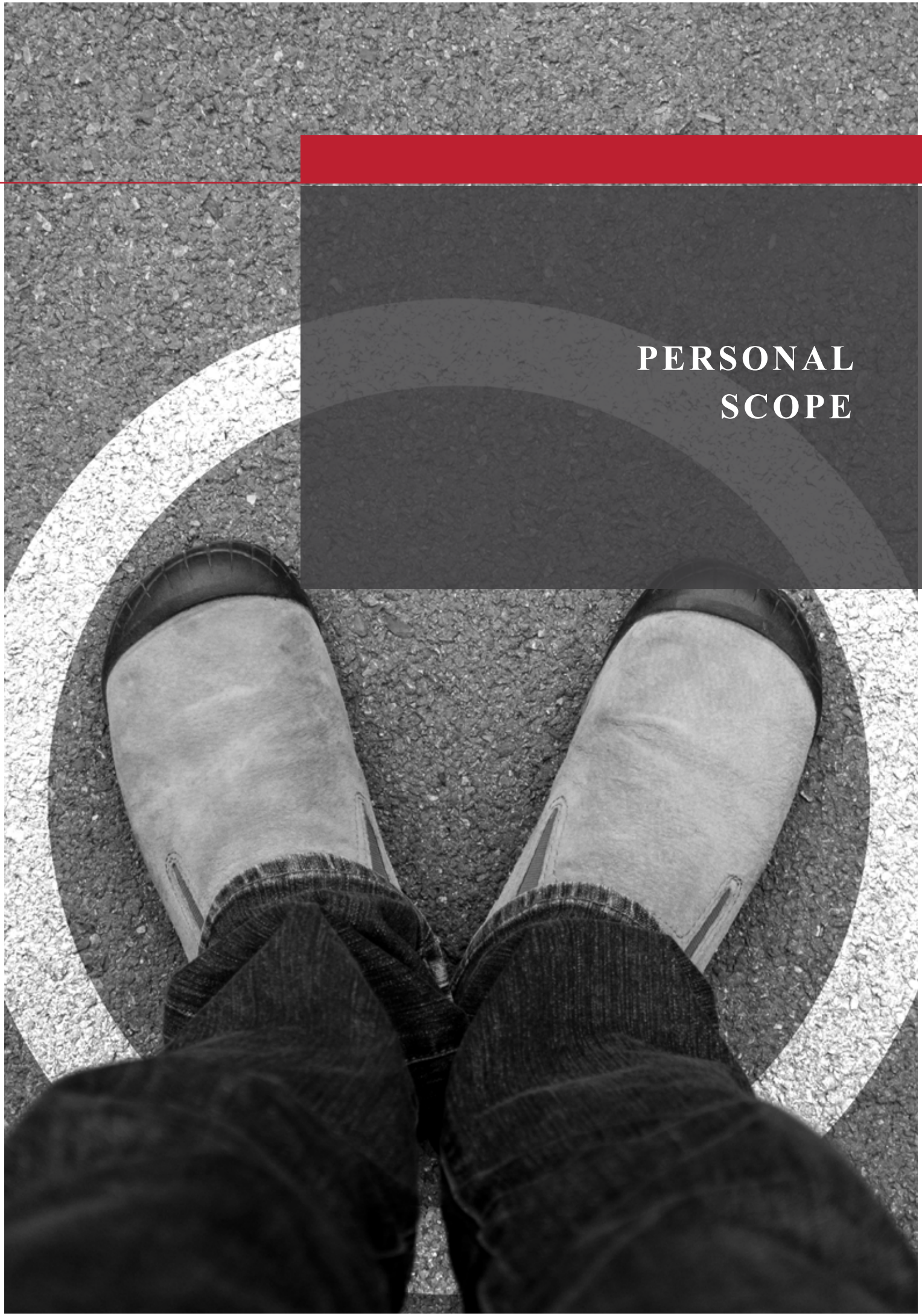
Data Sharing

In order to address the aspect of enforceability, the Proposed DP Law should prescribe certain minimum, non-negotiable terms to be included in the contract between: (i) the data subject and the entity collecting personal data; and (ii) such entity and any other person to whom such entity hands over the tasks of storage, use or processing of personal data. Such mandatory contractual terms could include a compulsory acceptance of Indian law and the jurisdiction of Indian courts/regulators.

Prospective Effect of Proposed DP Law

Any offence defined under the Proposed DP Law can be punished only if committed from the date on which the new law is made effective, even though such offences may relate to data collected prior to the enactment of the Proposed DP Law. This owes its origin to principles of retrospective application of criminal law under Article 20(1) of the Constitution of India. Therefore, provision of a transitory time for companies to come into compliance with the new law should be provided before the new standards and procedures for data protection are made completely enforceable.

PERSONAL SCOPE



Right to protection of personal data only extends to individuals. Personal data should be broadly defined. Any data which is reasonably sufficient to allow direct or indirect identification of an individual constitutes personal data. Data collected by non-human controlled data processing systems should also be covered under the definition.

As recognised under the European Union's GDPR, the concepts of privacy and autonomy are available only to natural persons and not companies. By affording constitutional protection to 'right of privacy', state instrumentalities have been made accountable to a greater degree in terms of data protection. Accordingly, it is suggested that the Proposed DP Law should provide protection for individuals against the State and its undertakings, as well as against privately-owned entities. For the purpose of protecting the interests of the State, the reasonable restrictions prescribed under Article 19 of the Indian Constitution may be extended even in cases of breach of privacy. It is also important to note that a company's valuable information, such as confidential information, trade secrets and intellectual property rights, are protected under contract law or intellectual property law, and therefore, it is submitted that there is no specific need to extend the Proposed DP Law to protecting a company's business information.

Personal Data

It is imperative that the definition of "personal data" or "personal information" *(irrespective of the nomenclature)* in the Proposed DP Law should be robust to meet the multiple ways in which technology is used to attract information. Modern technologies such as targeted online advertising, which make use of an individual's online activity trends to customise advertising, can be intrusive on a person's privacy and autonomy without actually accessing any "identifiable" information. This data may not be independently "identifiable", however, collectively such data may result in identifying an individual, thus being a violation of privacy. Technologies associated with artificial intelligence and internet of things may access individuals' data already present in various systems including computers, servers, cloud storage or on the internet, without such individuals actually delivering the data or even being aware that data is being collected or analysed. For this reason, the definition of "personal data" needs to be broad in its scope and application.

The term "personal data" needs to be defined widely, and to the extent possible, be technology-neutral. Any data or information that is reasonably sufficient to allow direct or indirect specific identification of an individual must be included within the definition.

Any information which in conjunction with other data helps to 'reasonably identify' an individual should be covered in the definition of personal data, regardless of whether the data was subject to anonymization or pseudonomyzation.

Further, in our view the definition of "personal data" must include both facts (such as name, age, address, etc.) as well as other data (such as credit score, online activity history, hobbies, interests, etc.) whether or not such data constitutes fact or opinion, whether or not there is an overt act of disclosure of data by an individual, and regardless of accuracy. Data collected by non-human controlled data processing systems, without the knowledge of a data subject, must also be included within the definition.

There may of course be certain exemptions from what is treated as personal data, on the grounds of sovereignty and integrity of the country, security interest and national peace. However, when personal data or personal information is shared with other regulators or law enforcement authorities under applicable law, there should be a specific obligation on such regulators or law enforcement authorities to keep the information confidential and take due care to ensure that it is not used for any purpose other than that which it has been collected.

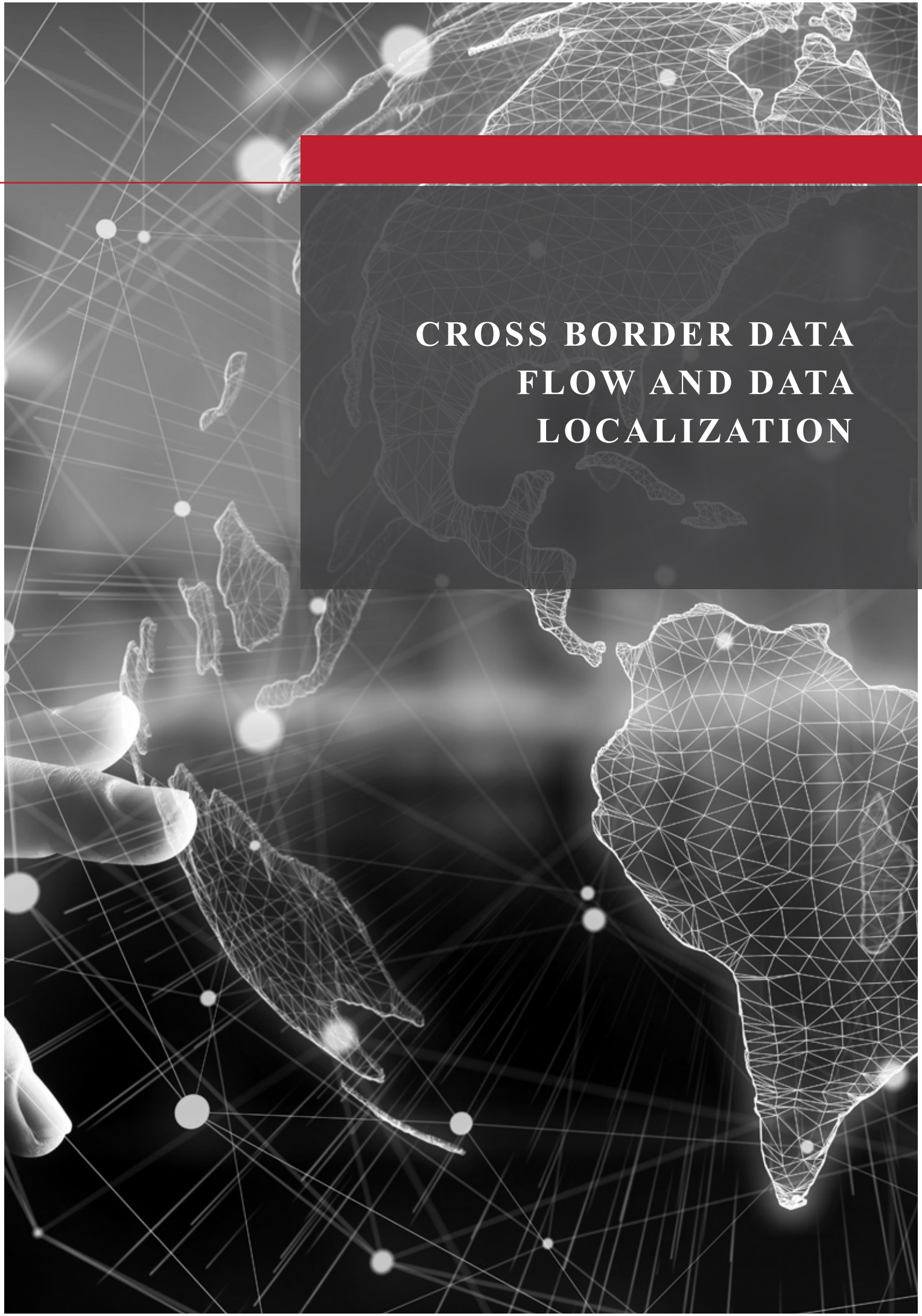
Sensitive Personal Data

Based on the definitions of "sensitive personal information" from various jurisdictions around the world, there seem to be two broad reasons why such sub-classification may be necessary: (i) some information is considered as being "intimate" or "extremely personal" to the individual; and (ii) such categories of data may be used to discriminate against an individual.

Any personal data including an individual's religion, race, caste, sexual orientation, marital status, health conditions, place of birth, descent or place of residence or such other details that the individual so designates may be presumed to be "sensitive". An individual should be given the option to refuse to divulge these details *(particularly since it may form the basis for discrimination)* unless it is quintessential for the purpose for which it is being sought. The disclosure of such information must be made voluntary on the part of the individual, and the forum interacting with an individual must not insist on disclosure of such information or make non-disclosure of such information the basis of rejecting the benefits sought by such individual.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 **("SPDI Rules")** defines six categories of information as being "sensitive personal data or information", and provides for rules relating to the collection, use, processing and disclosure/ transfer of such information. It is our view that this position be retained under the Proposed DP Law. In addition, it is suggested that biometric information, religion, race, caste, gender and criminal record be included under the definition of "sensitive personal information". In this context, the legislators may also consider creating certain reasonable exceptions, for e.g. disclosure of a record of offences involving moral turpitude when the individual is applying for a job involving care of children or elderly people.


assword
*****



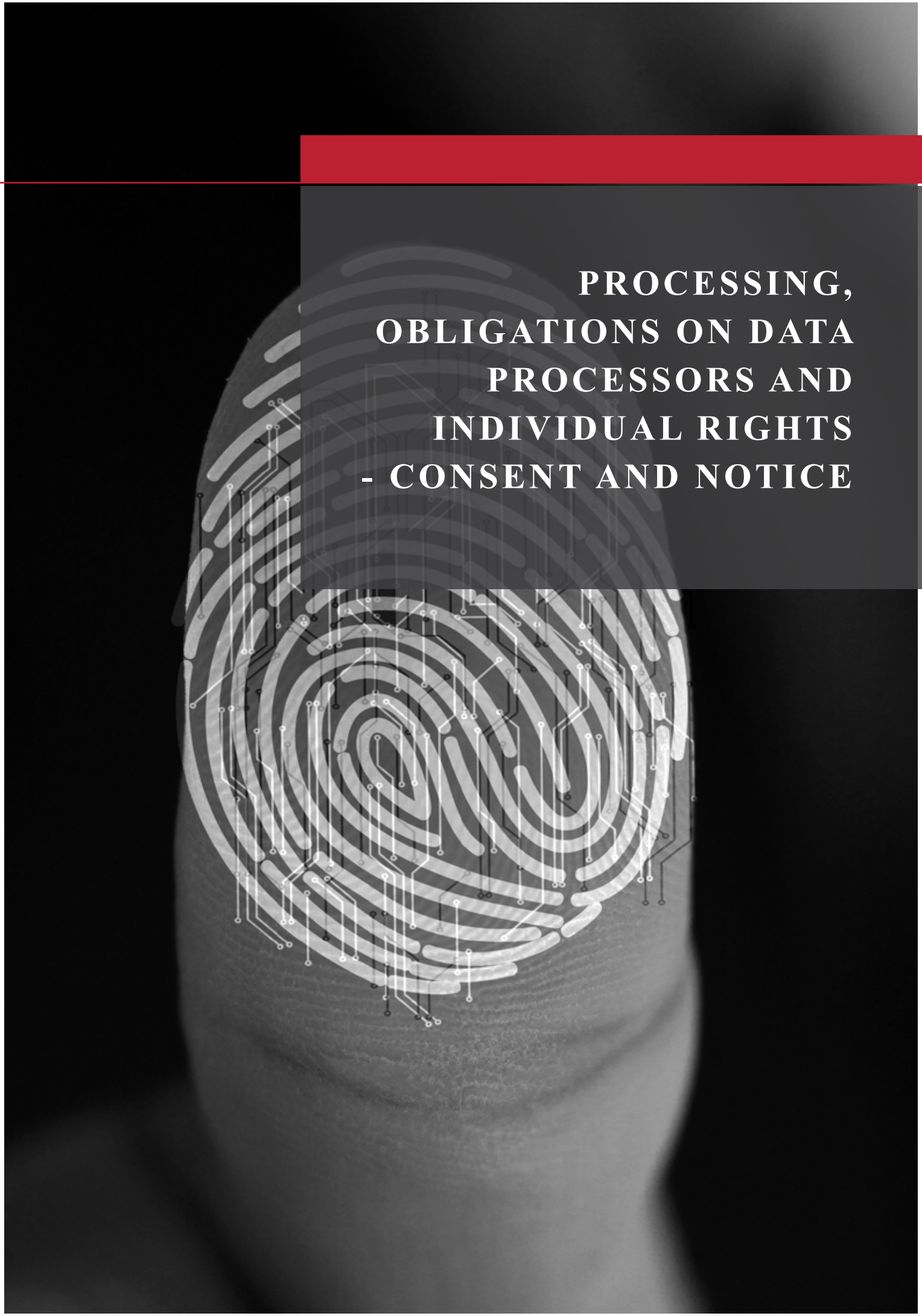
CROSS BORDER DATA FLOW AND DATA LOCALIZATION

Along with the "comparable level of protection" test, the "adequacy" test must also be implemented. Further, sensitive personal data should only be transferred outside the country, when absolutely necessary and some sensitive personal data that is required to be transferred out of India must still be located on a server or a datacentre within India.

The Proposed DP Law Law must cater to both (i) cross-border transfer of personal data of Indian data subjects; and (ii) cross-border receipt, and thereafter processing, of foreign data subjects in India. For this purpose, the standards specified for such transfer must be equivalent to or higher than those laid down in other countries with developed data protection regimes.

Transfer of sensitive personal data under the SPDI Rules is only permitted if the receiver (Indian or foreign) implements data security standards and procedures at least as stringent as in the Rules. Rule 8 of the SPDI Rules lays down the standards and procedures required to comply with the Rules, these must be checked against the most stringent requirements existing in other counties and any consequent gaps must be addressed. It is our view that the Indian Government must work with the foreign data protection regulators to have India recognized as a country that satisfies the legal requirements of that other country. Thus, along with the "comparable level of protection" test, the "adequacy" test must also be implemented.

In terms of cross-border transfers and data localisation, neither a blanket prohibition on cross-border transfer of personal data nor a blanket rule requiring localization of all personal data, are desirable or practical. A balance has to be struck between national interests and ease of doing business. In the interest of national security, sensitive personal data such as biometric information of Indian data subjects are not required to be transferred abroad in any reasonable business context, and such sensitive personal data must be kept within the country. Some sensitive personal data that is required to be transferred out of India must still be located on a server or a datacentre within India. This will also provide a resolution to the question of territorial jurisdiction of the Proposed DP Law.



PROCESSING, OBLIGATIONS ON DATA PROCESSORS AND INDIVIDUAL RIGHTS - CONSENT AND NOTICE

For free and valid consent a clear notice of the fact of collection and processing of data must be provided to the data subject along with the opportunity to clearly, transparently and explicitly signify consent. Implied consent, inactivity or pre-checked boxes signifying consent should not be acceptable modes of consent. This should equally apply to data collected through manual and through automated processes. Adopting a standard form of notice and outlining the type and method of data collection would be a cost – effective method for ensuring that the requirements of consent and notice (two pillars of right to privacy) are adequately met.

Privacy is closely associated with the autonomy and identity of an individual, as recognized in the Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCALE 1 (**"Puttuswamy Judgment"**) and the white paper. While consent need not be the sole basis for the processing of personal data, it should be one of the primary requirements for collection, processing and use of personal data. Business realities, unequal bargaining power and the development of new technologies often relegate the concept of "free consent" of an individual to the status of a legal assumption.

Thus, along with consent, the processing of data must be permissible only when the data processor needs to do so in order to fulfil a legal or contractual obligation, and such obligation cannot be fulfilled unless personal data in a regulated manner.

For free and valid consent, a clear notice of the fact of collection and processing of data must be provided to the data subject along with the opportunity to clearly, transparently and explicitly signify consent. This can be by way of a click wrap agreement but implied consent, inactivity or pre-checked boxes signifying consent should not be acceptable modes of consent. It is therefore important that the consents obtained are documented and retained for the period of collection, processing or use of personal data. The data subjects must also be allowed to withdraw consent.

There are sufficient safeguards for data collected through manual and human-controlled processes but organisations that may access or use personal data during an automated process, such as data analytics or data mining, must provide specific notice to this effect along with the purpose of collection and proposed use, and obtain their explicit prior consent.

Further, obtaining consent should not allow the data controller or data processor to disclaim all legal liabilities.

There are multitudes of business activities or purposes and personal data may be collected by various organisations which would lead to "multiplicity of notices" and a "consent fatigue". This practical difficulty should not be used as an argument to trivialize consent, in fact it strengthens the need for informing the data subject of the fact and purpose of collection and processing of personal data.

As a simple and cost-effective method, a standard form of notice can be adopted containing the (i) nature of personal data collected; and (ii) purpose of collection, processing and use of data. Simple English should be used and the main points should be ether in bold type face or in a different colour. It shouldn't be hidden away in a form of URL, etc. It may also be provided in Hindi or other regional language.

While consent is an important premise for the collection and processing of personal data, it is submitted that specifying different standards of notice and consent for different forms of personal data is both difficult to practically achieve and subject to the risk of obsolescence in light of fast-evolving technologies. At the same time, permitting the data controllers to make context-specific determinations of the applicable standards may result in lack of uniformity and adoption of insufficient standards. However, what the law can provide for is providing broad limits on the purposes for which sensitive personal data may be collected and processed and the manner of providing and documenting consent.

However, there is currently one glitch, the data subject can either (i) provide blanket consent to access all services offered by data controller; or (ii) not provide consent at all and in turn not access any of the services offered by data controllers.

They cannot selectively provide consent to access certain services offered by the data controllers. In the context of modern internet-enabled businesses and technologies, "notice and consent" aren't very straightforward.

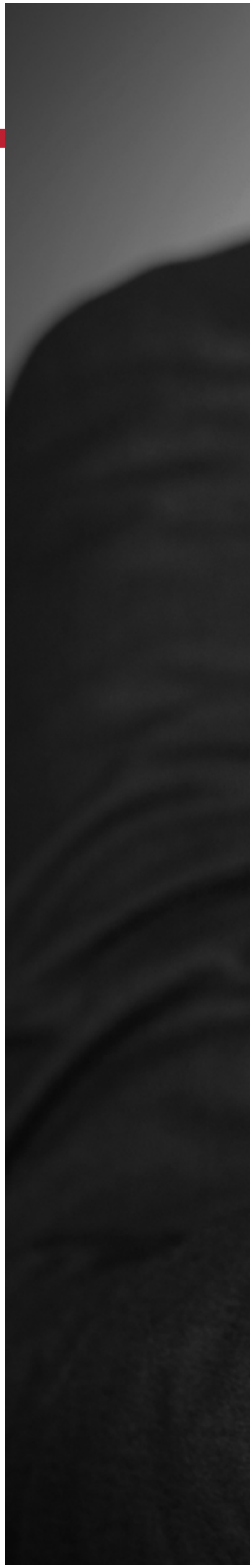
What might help are Privacy Impact Assessments ("PIA") which are to ensure that the most serious risks of privacy breaches are identified and addressed effectively but the mechanism and oversight of the same differs across jurisdictions. Some critical sectors or industries such as healthcare, finance, etc. must be identified for an initial phase of PIA rollout, as it can be expensive and time consuming.

The Proposed DP Law should consider inclusion of a "consent dashboard" which will give the data subjects the right to access their personal data and verify the lawfulness of processing and use. This will enable the data subjects to object to any unjustified use and allow the data subject to withdraw his/her consent, where necessary. This is however based on the presumptions that such data is traceable and accurately recorded, organisations upload and share such data into the dashboard and the entire cycle of collection, storage and processing happens through a human-controlled process.

In this regard, it is a concern that the consent dashboard itself may constitute "sensitive personal data" and must thus be put under the watch and control of an independent neutral regulator that is brought under the framework of the Proposed DP Law.

If it is maintained by a government entity, it should not be exempted from the applicable rules for the purpose compliance.

It is submitted that recognition of organisations with an excellent track record of compliance with privacy laws is important, and must also be supported by a system of reward in the form of lesser scrutiny from the regulator under normal circumstances. One such mechanism may be in the form of a "data trust score", for which criteria such as numbers of breaches, complaints and rectification requests, and also factors such as proactive provision of "notice and choice", transparency, ease of comprehension and robustness of information security systems, may be taken into account. Such score may be subject to annual review and revision, as necessary. The rules for calculation of such score may also differ according to the sector in which the organisation operates, and may be administered by the data protection regulator or a department constituted thereunder. Such a system will also increase faith in the overall framework of the Proposed DP Law, from the point of view of individuals and businesses alike.



PROCESSING, OBLIGATIONS ON DATA PROCESSORS AND INDIVIDUAL RIGHTS - PURPOSE SPECIFICATION AND USE LIMITATION

The future use must not be totally incompatible with or contrary to the originally stated purpose, and must be something that demonstrably has a reasonable and immediate nexus with the originally stated purpose.

A data subject while providing personal data can legitimately expect that it is only used for the furtherance of a specified, explicit and lawful purpose and not for anything else. Thus this purpose specification and use limitation cannot be done away with. It is equally important to ensure that the law is dynamic enough to encourage new technologies while providing a robust framework of security for and protection of individual privacy rights. There is a need to strike a balance through the test of reasonability. The future use must not be totally incompatible with or contrary to the originally stated purpose, and must be something that demonstrably has a reasonable and immediate nexus with the originally stated purpose. Further where initial notice does not provide clear insight into how data may be used in the future (e.g. in cases of "Big Data"), then it must be the data processor's obligation to provide fresh notice to the data subject regarding such new uses or purposes, and further processing must be subject to the individual's renewed explicit consent to the new purpose.

It would be important to identify specific sectors or industries, especially those which deal with sensitive personal data or information, and define strict adherence to the rules regarding purpose specification and use limitation. For example, where medical history is collected for treatment of a disease, the scope of use is limited and there is no 'reasonably foreseeable' future purpose for the use of this information. For this the data protection regulator may collaborate with the sectoral regulators.

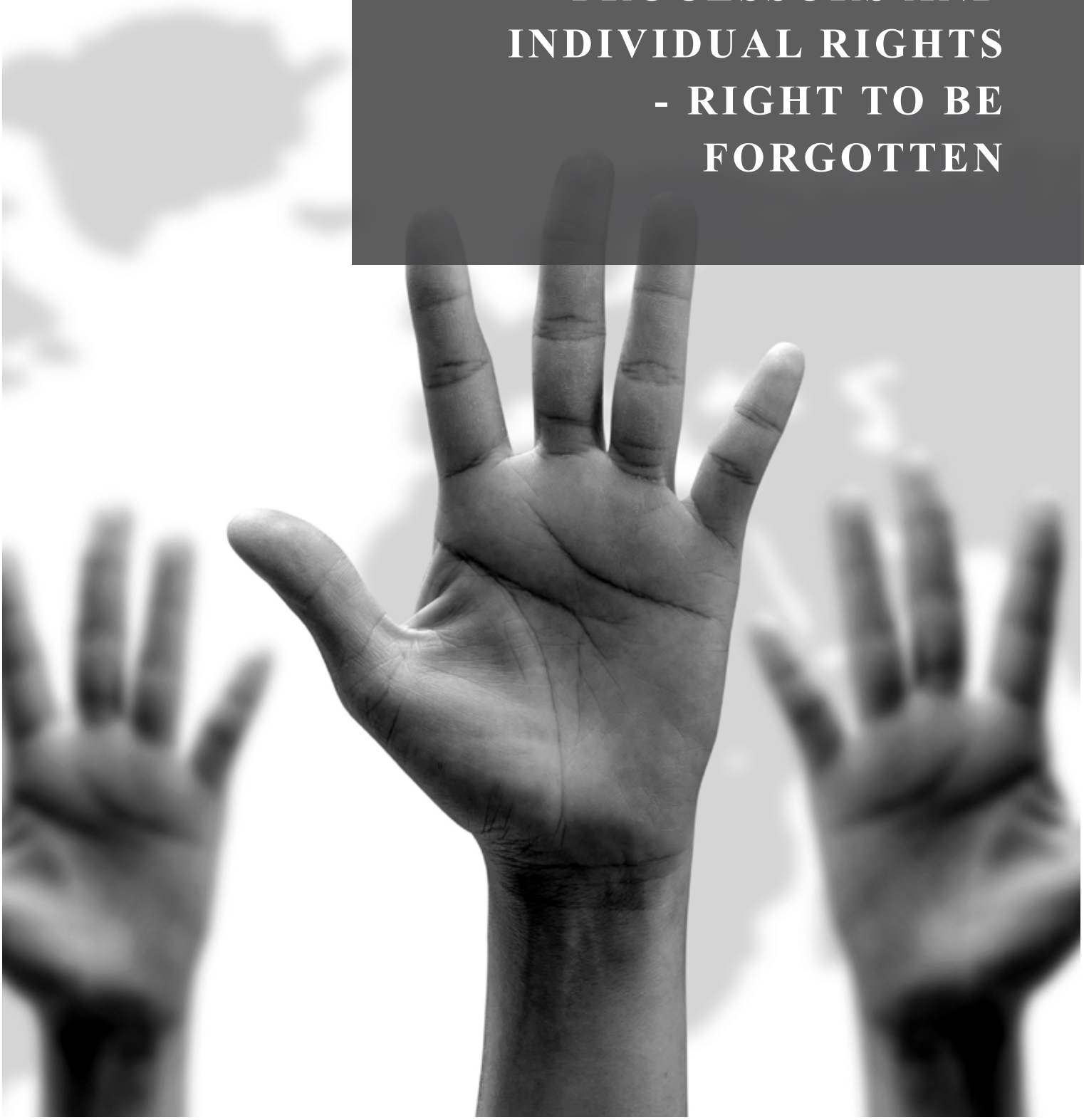
Further, broadly defined purposes, such as "improving user experience" or "marketing purposes" must not be permitted and there must be a reasonable nexus between the business or service offered by the organisation and the list of purposes stated in the notice to data subjects.

Individual Participation Rights

A data subject must always have the right to access and/or rectify personal data regardless of the mechanism of collection or storage, or the technology using which such data may have been collected or stored. However the personal data may be accessed or rectified only when the data controller has expressly and intentionally collected personal data, whereas such actions may not be even possible in the case of automatically collected data or "data trends". The view suggested in the white paper to levy a fee on an individual who wishes to access or rectify his/her personal data is practical and also serves to strike a balance between business considerations and individual rights.

For enforcement of such a right, an independent data regulator may be preferable and more accessible than a court of law and it may also be empowered to issue directions to data processors to provide access to or rectify an individual's personal data.

PROCESSING, OBLIGATIONS ON DATA PROCESSORS AND INDIVIDUAL RIGHTS - RIGHT TO BE FORGOTTEN



If the necessity of notice, consent, purpose specification and use limitation isn't followed in entirety or in part or the purpose has been achieved then in such instances a right to be forgotten may be given retrospective effect. The right to be forgotten must extend to all personal data, and not just sensitive personal data/information and must also extend to data collected by automated processes.

The right to be forgotten must be understood outside the scope of:

a. SPDI Rules which provide for an obligation on the data processor to not retain sensitive personal data or information once the purpose for which it has been obtained has been accomplished;

b. existing measures to protect a person's reputation, dignity and intellectual property;

c. laws which place personal information such as court decrees, etc. in public domain;

d. instances of public interest or national security which warrant the data to be continued to be stored; and

e. information in public domain protected by right to free speech or exceptions to tort such as truth.

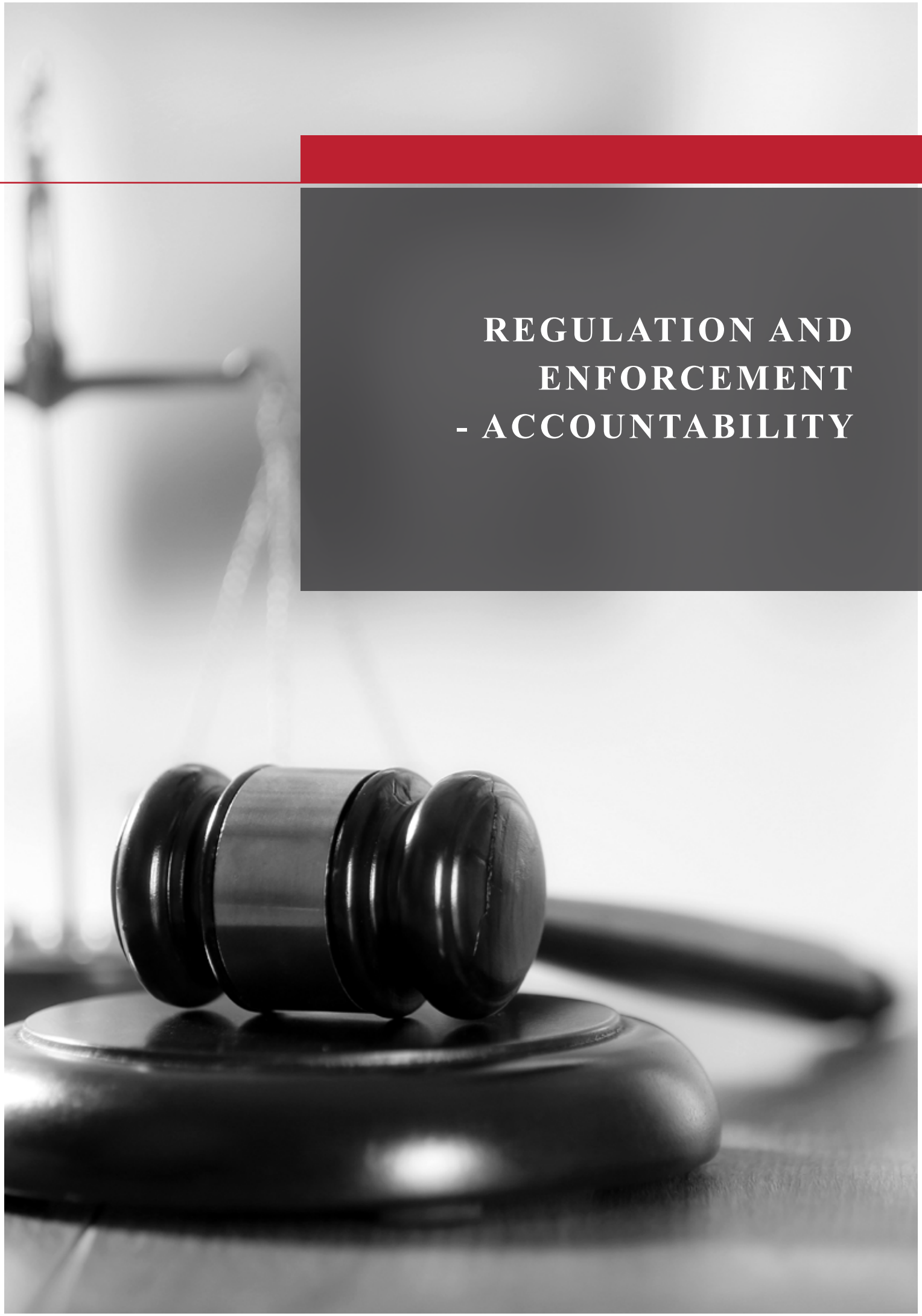
One facet of this has already been incorporated in the SPDI Rules wherein the data subject has a right to withdraw consent for his/her sensitive personal data or information from being further collected or processed.

It is also possible that the data subject doesn't consent to transfer of data and this right would thus work in the context of transferring personal data to another entity.

If the necessity of notice, consent, purpose specification and use limitation isn't followed in entirety or in part or the purpose has been achieved then in such instances a right to be forgotten may be given retrospective effect. The Proposed DP Law must clearly state the grounds for such a request and a request not made on the basis of these would be liable to be denied. It must be applicable to all personal data not just sensitive personal data/information. Further data may also be collected by automated processes where the data subject is not aware about the same. Irrespective of this, the right to be forgotten must exist for such data as well.

The Puttaswamy Judgement and the decision of the Karnataka High Court in Sri Vasunathan v. The Registrar General (2017 SCC OnLine Kar 424) referred to in the white paper discuss the right to be forgotten only from the context of deletion of personal data. Like other countries, as examined by the white paper, the right to further dissemination must also be included in right to be forgotten. Deletion might not be possible in instances where it has been widely disseminated in the online space or resident as "passive" data in servers beyond the data processor's control. In such a scenario, it is important to ensure that the data processor takes all steps to ensure that such data does not get further disseminated or transferred to any other person.

REGULATION AND ENFORCEMENT - ACCOUNTABILITY



Both, data controllers and data processors should adopt specific measures to demonstrate accountability, based on standards and regulations which would be general and sector-specific, and should have liability affixed, in case of data breach. The nature and extent of liability should depend on the nature of data, the party responsible for handling data and the measures adopted. Data controllers should mandatorily be required to obtain insurance policies and adopt a risk management mechanism to mitigate loss due to data breach.

The European Union based on the principle of accountability requires data controllers to address two important facets: implementation of data protection principles after identifying them and demonstration of such implementation if required by a supervisory authority in order to ensure greater accountability for the data controller.

As for organisational standards to be adopted, the Proposed DP Law should contain specific rules (including specific criteria for duty of care) to enable data controllers to demonstrate accountability. Factors such as current technology standards, sector specific requirements and nature and quantum of personal data being handled must be taken care of in the legislation so as to make it technology compliant. Moreover, strict consequences for failure to adhere to these standards must be prescribed.

It is our view that sector-specific regulators should also consider prescribing additional guidelines or compliances to be undertaken by data controllers.

In case of a conflict, the sector-specific rules should prevail over general ones. In terms of penalty, there should not be any restriction on a data controller under the Proposed DP Law as well as under sector specific guidelines. Notwithstanding the aforementioned, the principles under the Evidence Act, 1972 would be applicable for the data controller to prove that it fulfilled its duty of care to prevent or mitigate data breach. This will help in determining the liability of the data controller during adjudication for a data breach.

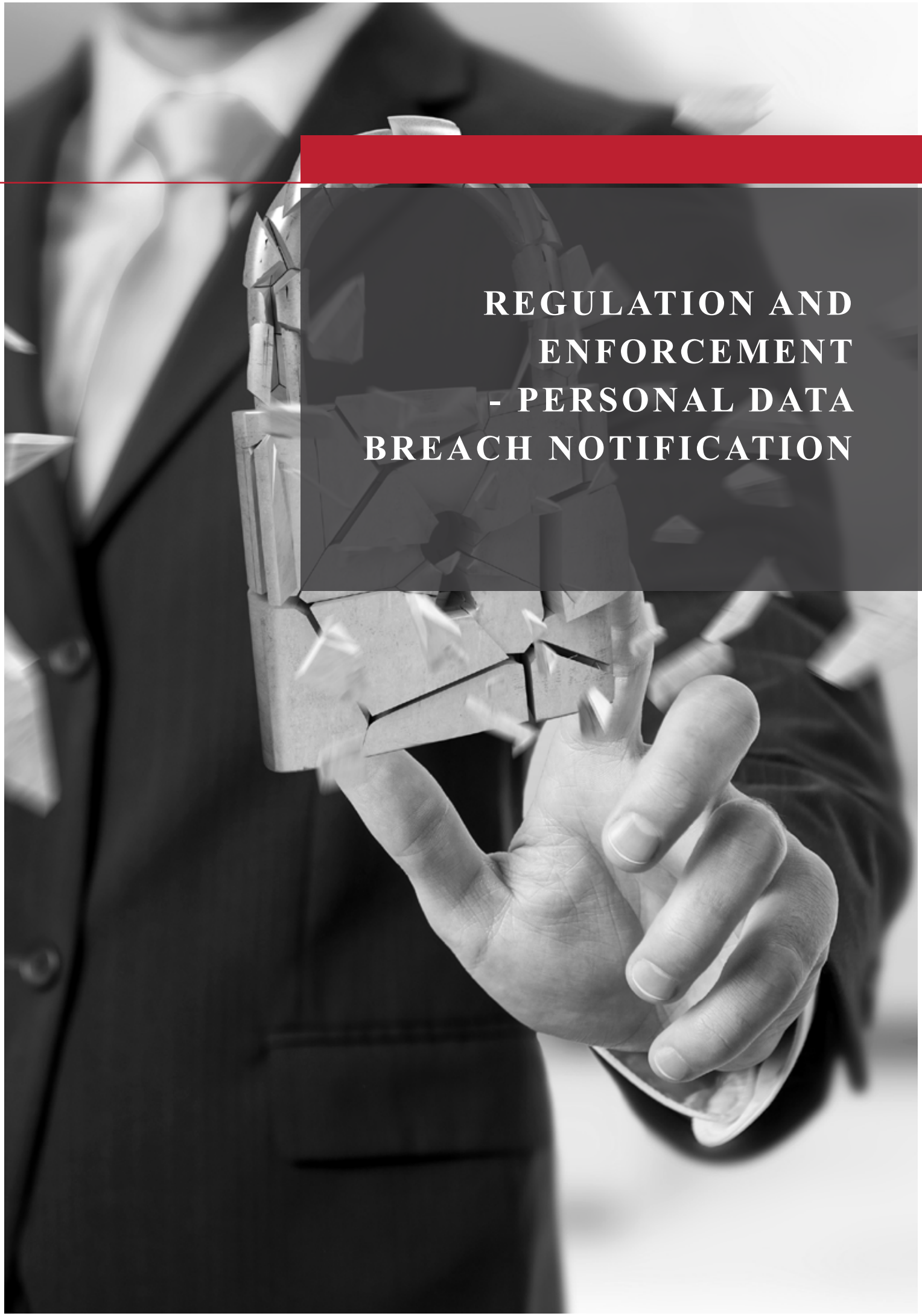
In this regard, there are two kinds of data breach: (a) owing to technological failure and (b) owing to fault, whether negligent or wilful. As for the former, the person responsible for collecting and handling data i.e. a data controller, should be held responsible, however, there should be an option to cap such liability to the extent that there is evidence to establish that it took adequate measures to prevent the breach. In such instances, no penalty should be levied on the data controller. As for the latter, the person responsible should be held accountable to a greater degree and be liable to compensate the individual as well as pay the penalty subject to no cap on the compensation or penalty. Breach under both categories should include both objective and subjective harm so as to offer a spectrum of possibilities for which the individual can seek remedy or compensation.

In this context, it is relevant to analyse Section 79 of the Information Technology Act, 2000 which exempts intermediaries from liability in certain cases. The exemption from Section 79 should not extend to the specific event contemplated above and for this reason it would be necessary to amend Section 79 to this limited extent.

Given that modern data processing is complex and may involve several persons, it is difficult to enjoin any one person with the liability for data breach, and therefore the data controller should be ultimately responsible and accountable for the data.

However, the data controller can seek indemnities or affix contractual liability to third parties involved in data processing ensuring strict compliance. In this context, it is suggested that the Proposed DP Law specify certain guidelines/standards for data controllers to appoint data processors and also exercise due diligence in this regard

Moreover, data controllers should mandatorily be required to obtain insurance policies commensurate with the quantum of data handled by them as well as the sector in which such data controllers operate, covering any and all liability in case of data breach. This is to ensure enforcement of the claim of an aggrieved person as against the data controller. Besides being accountable, the data controllers should have a system in place to prevent, detect and react to data breach and mitigate associated risks including adopting interim measures.



REGULATION AND ENFORCEMENT - PERSONAL DATA BREACH NOTIFICATION

Identification of the nature of breach is important especially in the cases of personal data breach whereby a timely notification to the relevant individual and proper reporting to the Authority will help in mitigating the damage caused by it.

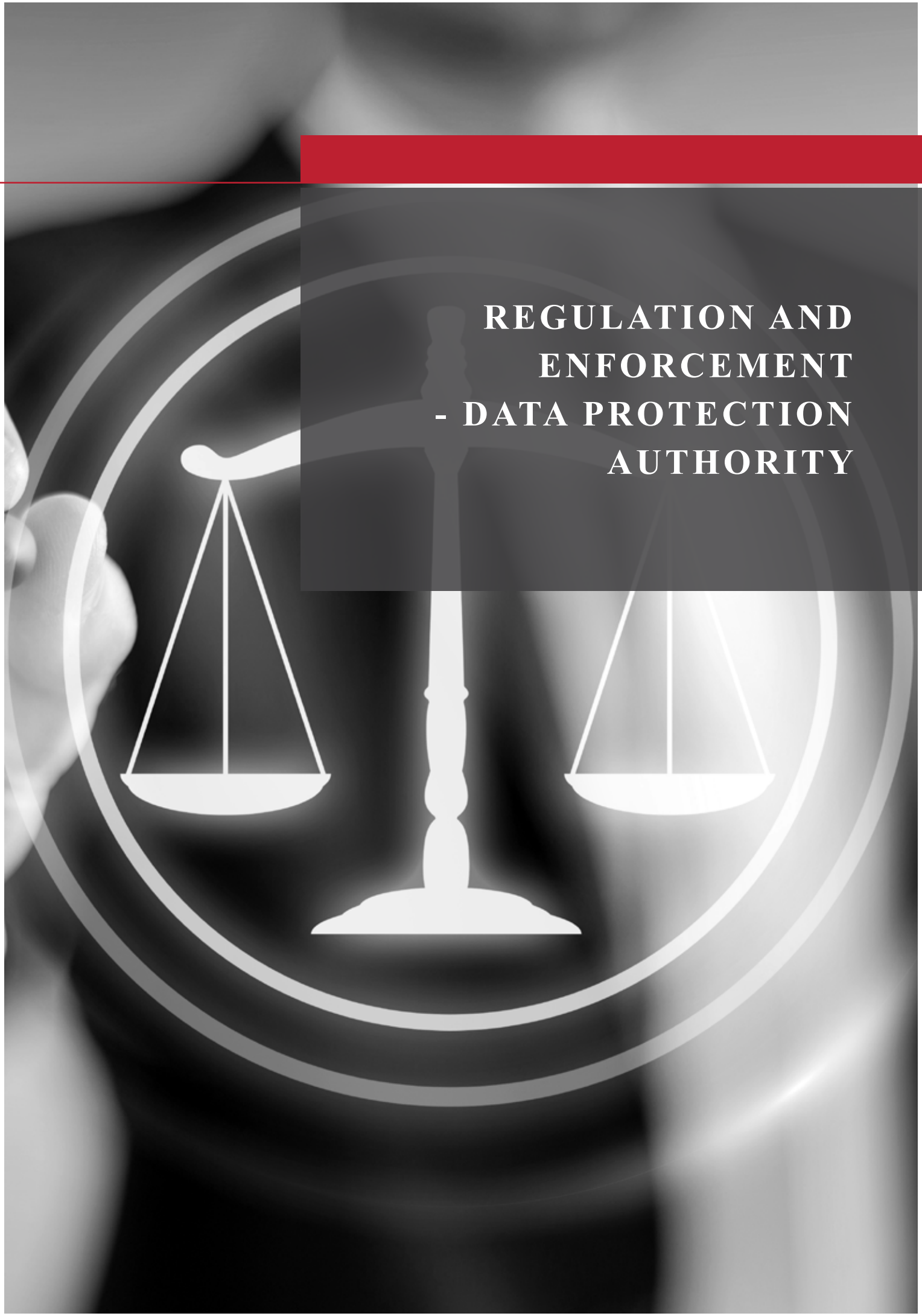
There are three internationally recognised forms in which a personal data breach may occur – confidentiality breach, integrity breach and availability breach.

The European Union's GDPR defines a personal data breach to include all these forms of breach, but defines a personal data breach as a "security breach".

The white paper discusses the practical difficulties in both identification and notification of a personal data breach and how all security breaches need not necessarily be personal data breaches. However, persons or organisations managing or storing personal data would be typically be aware of the nature of the security breach and the likelihood of data controlled by it to be affected by the breach.

Hence, the data controller/processor should send out a notification in case of any breach and its likely effect upon the data.

The timing of the notification may depend on several factors such as whether it is sensitive personal data, the number of individuals affected, nature of breach, etc. The content of the notification may be standardised by providing a form in the Proposed DP Law. It may entail basic details to the individuals such as the time of breach and the kinds of personal data under threat. The notification to the Authority/regulator must additionally include greater details with regard to the breach including the mitigation strategy of the organisation.



REGULATION AND ENFORCEMENT - DATA PROTECTION AUTHORITY

An independent dedicated Authority having a specialised structure is significant for an efficient adjudication and disposal of data privacy issues.

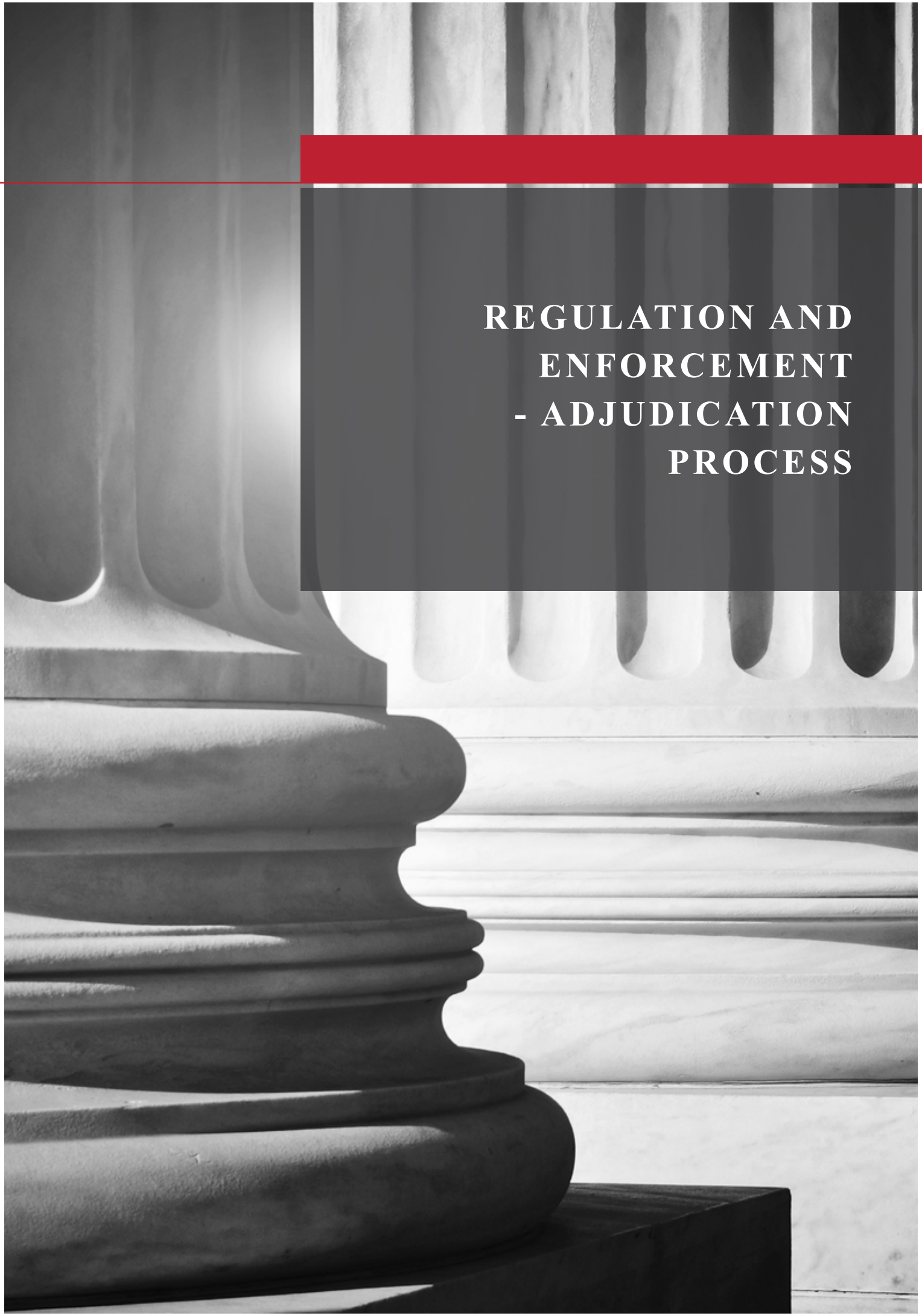
The white paper suggests that there should be a separate and independent authority under the Proposed DP Law. The issue of personal data breach involves issues relating to privacy which is a fundamental right. Further, personal data breach has a grave and immediate negative effect on the concerned individual. Thus, a special and dedicated body is necessary to adjudicate issues relating to it than submitting to the jurisdiction of the existing overburdened judiciary.

It is important that the authority is independent so as to have an efficient system of enforcement. It is also important to ensure that the data protection authority: (i) is staffed by persons of adequate qualification; (ii) has sufficient jurisdiction and power to adjudicate disputes (including by way of taking suo moto action) and issue binding orders; (iii) has quasi-legislative functions to not only determine standards, but also prescribe rules and procedures concerning the operation of the law; (iv) has the authority to monitor compliance with the applicable laws and procedures; and (v) can perform to a great degree of independence from government intervention or influence.

It is our view that the Authority should be centrally headed by the National Data Protection Commissioner who should be given a constitutional status like that of the Comptroller and Auditor General of India, for privacy is a fundamental right.

Furthermore, the National Data Protection Commission should ideally have separate departments established under it, each performing key functions, including: (i) legislative, advisory and investigative functions as well as technical recommendations; and (ii) judicial functions such as enforcement and dispute resolution. However, a number of functions, such as standards setting and prescription of standard forms and notices, may be performed by the authority in consultation with subject-matter experts as well as industry groups. This will ensure that standards and rules are evolving along with changing technology, while also keeping the interests of businesses in mind.

The Proposed DP Law must also differentiate between penalty/fine and compensation. The penalty amount is to be retained with the Authority whereas the compensation is to be awarded to the aggrieved person. The circumstances for both must be laid down clearly in the proposed legislation.



REGULATION AND ENFORCEMENT - ADJUDICATION PROCESS

The proposed Authority must be dedicated to alleviating issues from the individuals' end, enabling a class-action if required, by way of both pecuniary and subject-matter jurisdiction. Besides, presence of technical experts is essential on the panel adjudicating complex technological issues of data breach.

The data protection authority in the Proposed DP Law must have a judicial wing. The judicial body under the Proposed DP Law must be an independently appointed tribunal having exclusive jurisdiction over matters involving data protection or privacy. Such tribunal must have jurisdiction only to hear individual complaints, thus clearly excluding companies/juristic entities from addressing their grievances/complaints. This is important since the Proposed DP Law is about the protection of individuals' fundamental right to privacy. There should be a provision for class-action suits where a data breach affects a large number of individuals. Aggrieved persons can jointly seek remedy and the adjudicating process can award damages and penalise the data controller based on the nature and extent of data breach. Additionally, this would also be time efficient since matters concerning multiple data breaches by an entity can be adjudicated collectively.

While the Proposed DP Law may specify the pecuniary jurisdiction of the tribunals, the total compensation or monetary penalties that may be awarded/ imposed by the data protection tribunals must not be limited or capped by statute.

Furthermore, the tribunal should be staffed by officers having legal as well as technical expertise. This is common in the technology industry wherein the contracting parties insist upon the presence of a technically qualified person on an arbitral tribunal. The adjudication process should also permit video-conferencing as an accepted means of producing evidence and examining witnesses.

AUTHORS

Suneeth Katarki
Partner

Namita Viswanath
Partner

Nikita Hemmige
Associate

CONTACT US

BANGALORE
101, 1st Floor, "Embassy Classic"
11, Vittal Mallya Road
Bangalore 560 001
T: +91 80 4072 6600
F: +91 80 4072 6666
E: bangalore@induslaw.com

DELHI
2nd Floor, Block D, The MIRA
Mathura Road, Ishwar Nagar
New Delhi 110 065
T: +91 11 4782 1000
F: +91 11 4782 1097
E: delhi@induslaw.com

HYDERABAD
204, Ashoka Capitol
Road No.2, Banjarahills
Hyderabad 500 034, India
T: +91 40 4026 4624
F: +91 40 4004 0979
E: hyderabad@induslaw.com

MUMBAI
1002A, Indiabulls Finance Centre
Senapati Bapat Marg, Elphinstone Road
Mumbai 400 013, India
T: +91 22 4920 7200
F: +91 22 4920 7299
E: mumbai@induslaw.com

Disclaimer
This alert is for information purposes only. Nothing contained herein is, purports to be, or is intended as legal advice and you should seek legal advice before you act on any information or view expressed herein. Although we have endeavored to accurately reflect the subject matter of this alert, we make no representation or warranty, express or implied, in any manner whatsoever in connection with the contents of this alert. No recipient of this alert should construe this alert as an attempt to solicit business in any manner whatsoever.