Deloitte.

Privacy and Data Protection

Draft Personal Data Protection Bill 2019: A Summary

For Private Circulation Only | December 2019

Risk Advisory

Introduction

Protection of personal data of data principal* is at the core of the draft Personal Data Protection Bill, 2018 (hereafter referred to as “PDPB” or “bill”).

The Personal Data Protection Bill, 2019 released on 10 December 2019 introduced key changes from its draft version which was released last year on 27 July 2018 (referred to as PDPB 2018). Post approval by the Union Cabinet, the India Personal Data Protection Bill, 2019 (PDPB 2019) was introduced in the Lok Sabha (Parliament) by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019.

It was decided to refer the Bill to a Parliamentary Select Committee for review. Post this review the India PDPB 2019 will be introduced in the Budget session (tentatively in first week of Feb 2020).

This means once the bill is enacted and enforced, privacy will no longer be optional and cannot be ignored. Among many significant provisions, the PDPB proposes substantial penalty for violation of the stated requirements.

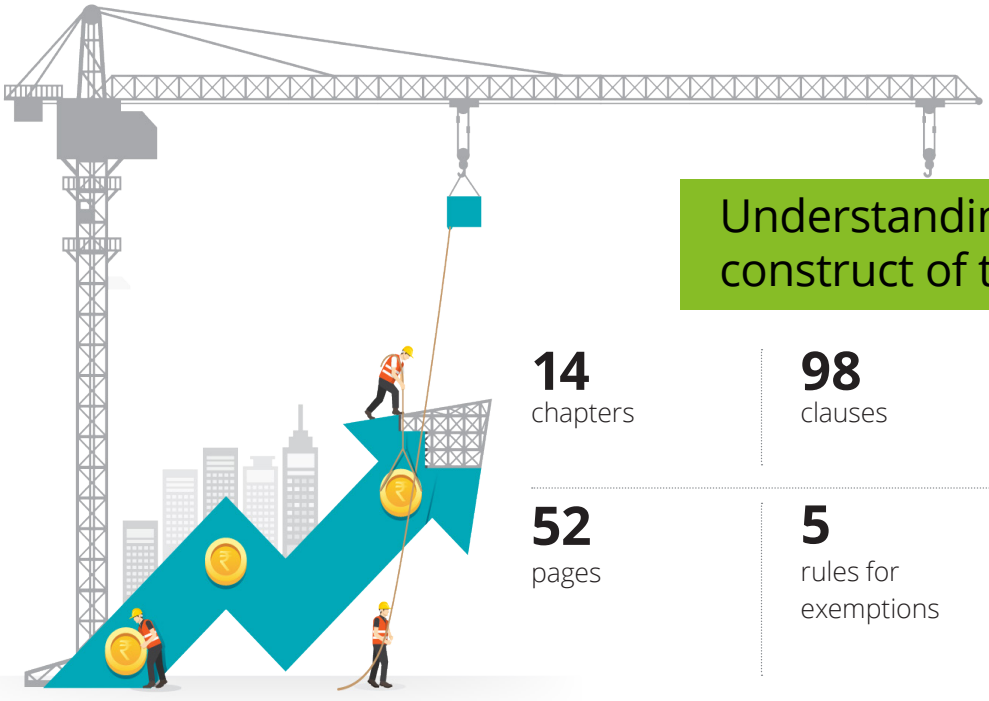
Such provisions along with heightened focus on collection and use of personal data, will require organisations (referred in the bill as Data Fiduciary and Data Processor) to revisit their risk acceptance criteria and establish a robust privacy and data protection framework.

The right to privacy makes protection of personal data utmost important

Changing global digital landscape in the 21st century

A legal framework for personal data not only for India, but for Indians

Need for a data protection reform to enable a free and fair digital economy



Understanding the construct of the bill

14 chapters

98 clauses

4 Rights offered for Data Principals / Individuals

52 pages

5 rules for exemptions

3 Months from the notified date for the Data Protection Authority to be established by the central government

Key propositions from the draft bill

Data Protection Authority of India
Bill proposes to establish an independent authority to oversee the enforcement of the provisions of the Bill.

Individual Rights
Bill proposes certain rights for data principals such as Right to access and confirmation, Right to be forgotten etc.

Territorial coverage beyond India to organisations processing the personal data, that have a connection with any business carried on in the territory of India or with any activity which involves the profiling of data principals within the territory of India.

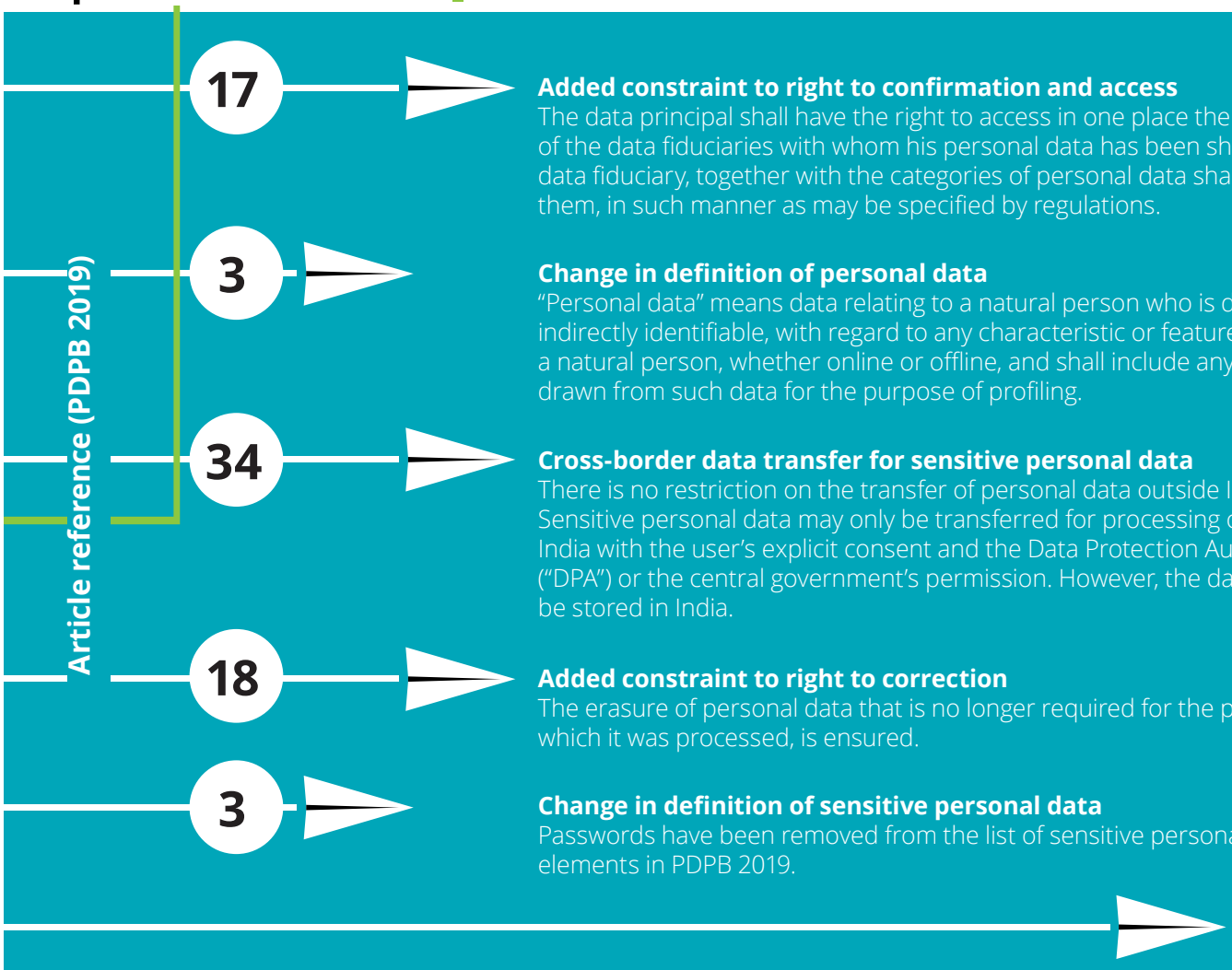
Data Localisation The 2019 version of PDPB has put an end on the blanket data localisation. The necessity of storing at least one serving copy in a data centre located in India has been done away with.
There is no restriction on transfer of personal data outside India, however, sensitive personal data may only be transferred for processing outside India with the user's explicit consent and the Data Protection Authority's ("DPA") or Central government's permission, but can only be stored in India.
Critical personal data has not been defined and will be defined vide a notification by the Central government, this type of data can be processed only in India.

Social Media Intermediaries
Social media with a certain high volume of users and ability to impact electoral democracy, India's security, sovereignty or public order, can be notified by the Central government and DPA as a significant data fiduciary (Entities processing high volumes of sensitive data).

Penalties of upto to Rs. 15 Cr (~USD 2.25M) or 4% of total worldwide turnover.

Changes to select provisions

After the approval of the Union Cabinet, the Personal Data Protection Bill, 2019 (PDPB 2019) was introduced in the Lok Sabha (Parliament) on 11 December 2019. The Lok Sabha decided to refer the bill to a committee selected by the parliament for review. Following this review, PDPB 2019 will be introduced in the Budget session (tentatively in the first week of Feb 2020).
The bill has three broad differences from its draft version: changes to select provisions; insertions of additional requirements; and deletions from the earlier version of the bill.



Added constraint to right to confirmation and access
The data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary, together with the categories of personal data shared with them, in such manner as may be specified by regulations.

Change in definition of personal data
"Personal data" means data relating to a natural person who is directly or indirectly identifiable, with regard to any characteristic or feature of such a natural person, whether online or offline, and shall include any inference drawn from such data for the purpose of profiling.

Cross-border data transfer for sensitive personal data
There is no restriction on the transfer of personal data outside India. Sensitive personal data may only be transferred for processing outside India with the user's explicit consent and the Data Protection Authority's ("DPA") or the central government's permission. However, the data can only be stored in India.

Added constraint to right to correction
The erasure of personal data that is no longer required for the purpose for which it was processed, is ensured.

Change in definition of sensitive personal data
Passwords have been removed from the list of sensitive personal data elements in PDPB 2019.

New additions

40

Sandbox
For the purpose of encouraging innovation in artificial intelligence, machine learning, or any other emerging technology in public interest, the authority shall create a Sandbox.

22

Privacy by design policy
Every data fiduciary shall prepare a privacy by design policy. Subject to the regulations made by the authority, the data fiduciary may submit its policy prepared under point (1) to the authority for certification within a period and manner specified by regulations. The authority or an officer authorised by it, shall certify the privacy by design policy after verifying that it complies with the requirements in point (1). The policy certified under sub-section (3) shall be published on the data fiduciary's website and the authority.

91 **Act to promote framing of policies for digital economy, etc.**
The 2018 draft provided for power of the central government to formulate appropriate policies for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such policies do not govern personal data. In the 2019 version, the central government, in consultation with DPA, may direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable the better targeting of delivery of services or formulation of evidence-based policies by the central government.

34 **Conditions for transfer of personal and sensitive personal data**
The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such a transfer, and where—(a) the transfer is made pursuant to a contract or intra-group scheme approved by the authority; (b) the central government, after consultation with the authority, has allowed the transfer to a country or, such an entity or class of entity in a country or, an international organisation; (c) the authority has allowed the transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose.

59

Penalties and compensation
When any provisions referred to in this section has been contravened by the state, the maximum penalty shall not exceed INR 5 crore under sub-section (1) and INR 15 crore under sub-section (2), respectively.

3 **Definitions**
A consent manager is defined as a data fiduciary that enables a data principal to gain, withdraw, review, and manage his/her consent through an accessible, transparent, and interoperable platform. In writing includes any communication in an electronic format as defined in the clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000. Data auditor means an independent data auditor and regulations mean rules made by the authority under this act.

28

Verification
Social media intermediaries classified as significant data fiduciaries will now have to give account verification options to willing users. The said verification has to be in the form of a visible mark of verification. The verification process will be voluntary.

26 **Social media intermediary**
With a large user base and ability to affect electoral democracy, India's security, sovereignty or public order, social media can be notified by the central government and DPA as a significant data fiduciary (entities processing high volumes of sensitive data).

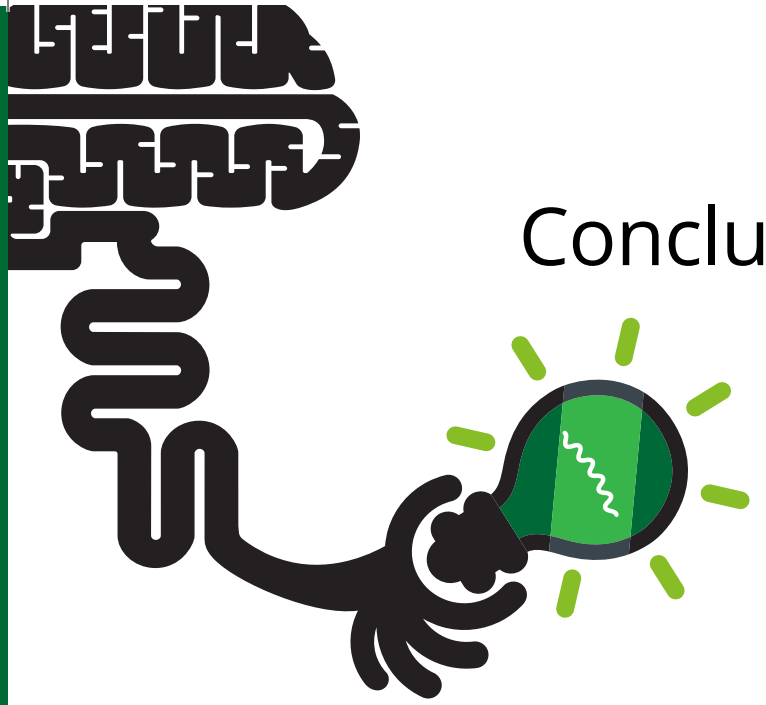
Key deletions

Accountability from article 11
Accountability includes the following:
The data fiduciary should be able to demonstrate that any processing undertaken by it or on its behalf is in line with the provisions of this act.

Every data fiduciary shall ensure the storage on a server or data centre located in India, of at least one serving copy of personal data to which this act applies. (Article 40)
The 2019 version of PDPB has put an end on the blanket data localisation. Now, storing at least one serving copy in a data centre located in India is not required.

Definitions of harm, significant harm, and data processor from Article 3
Harm includes:
(i) bodily or mental injury; (ii) loss, distortion, or theft of identity; (iii) financial loss or loss of property, (iv) loss of reputation or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement, or any other action arising out of a fear of being observed or surveilled; (x) any observation or surveillance that is not reasonably expected by the data principal.
Significant harm means harm that has an aggravated effect on the nature of personal data being processed, the impact, continuity, persistence, or irreversibility of the harm.
Data processor means any person, including the state, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary.

Conclusive remarks



1 The Personal Data Protection Bill seeks to lay down a framework to reserve the inviolability of consent in data transfer and processing. It also proposed to penalise those breaching privacy norms. It allows the processing of an individual's data only for lawful purposes.

The bill compels data fiduciaries to start processing data in India. Due to such a high level of data consumption, India is likely to become one the biggest centres of data refinery in the future.

2 Given that India does not have a defined framework that insures the protection of an individual's data, the bill is essential. PBPB will ensure confidentiality across sectors and will not be limited to a particular sector.

3 The robust framework is likely to promote 'privacy, the fundamental right for data principal', and enhance India's data sovereignty status because of proposed limitations sensitive personal data outside India.

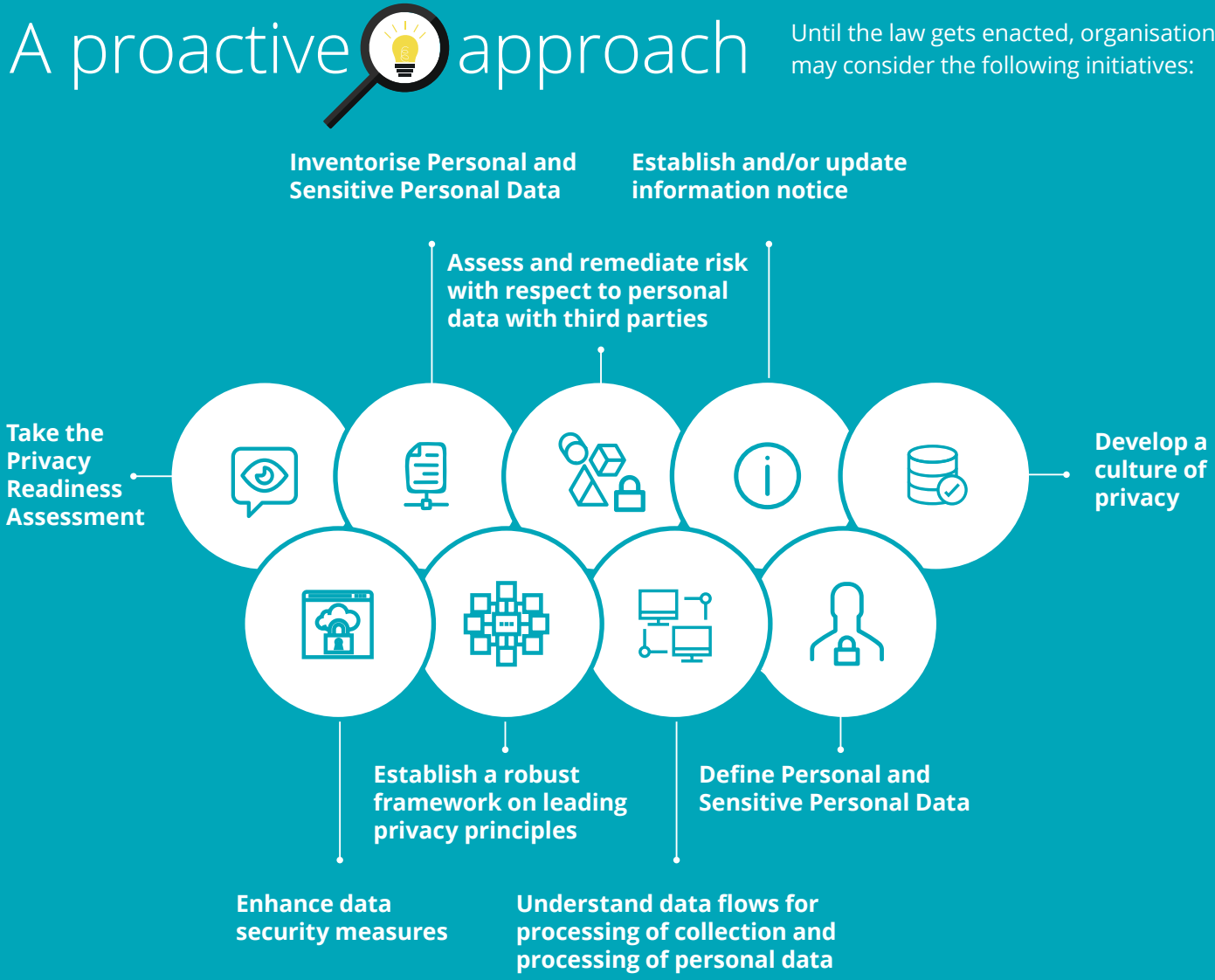
4 The government has segregated data as sensitive, critical, personal, and non personal, rather than putting it in one bucket. This will empower citizens to have an uninterrupted digital experience, while knowing that data will be collected, used, stored, and protected under a strict guideline.

Per PDPB 2019, data principal means a natural person to whom personal data relates; data fiduciary means any person, including the state, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing personal data; data processor means any person, including the state, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary.

What next?

A proactive approach

Until the law gets enacted, organisations may consider the following initiatives:



Implications

Penalty will be imposed if the following obligations are violated:

INR 15 cr or **4%** of global turnover, whichever is higher

01 Prompt action in response to a data security breach

02 Undertaking a data protection impact assessment by a significant data fiduciary

03 Conducting a data audit by a significant data fiduciary

04 Appointment of a data protection officer by a significant data fiduciary

05 Failure to register with the Authority

INR 5 cr or **2%** of global turnover, whichever is higher

01 Ground of processing of personal data

02 Ground of processing of sensitive personal data

03 Ground of processing of personal and sensitive personal data of children

04 Adhering to data security safeguards

05 Transfer of personal data outside India subject to defined conditions

Glossary

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

Data principal
means the natural person to whom the personal data relates

Data processor
means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary;

Personal data
means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling

Privacy is a fundamental right and protecting the personal data of Indian data principal is at the core of the bill.

Key contacts

National

Rohit Mahajan
President
Risk Advisory
rmahajan@deloitte.com

Shree Parthasarathy
Partner
Risk Advisory
sparthasarathy@deloitte.com

Manish Sehgal
Partner
Risk Advisory
masehgal@deloitte.com

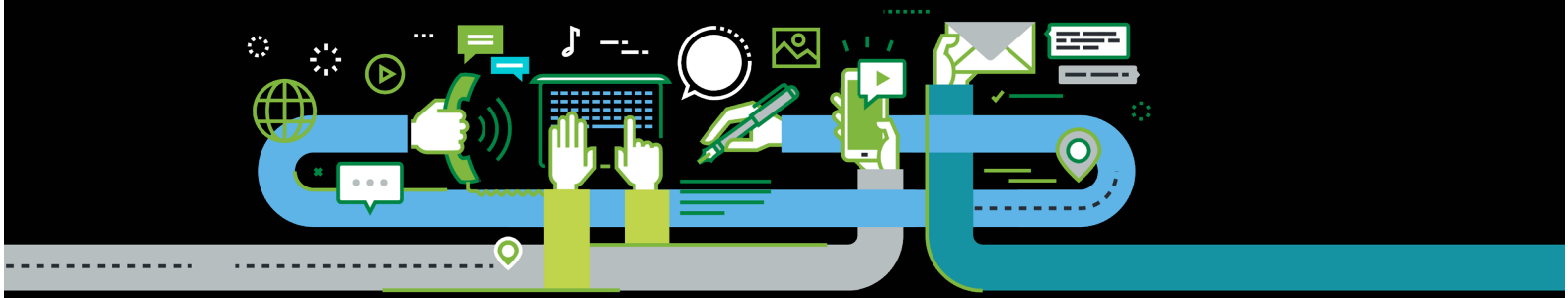
Regional

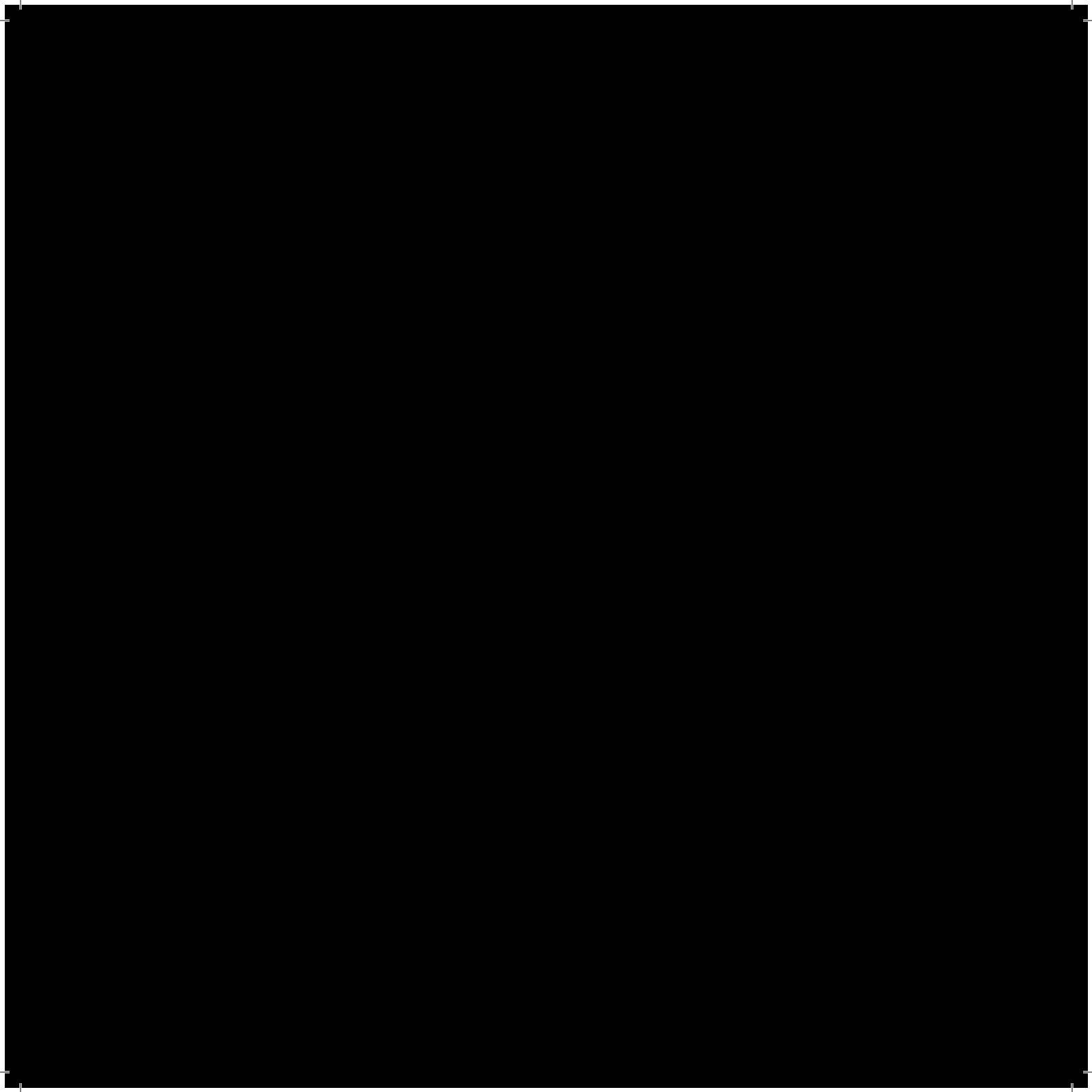
West - Ashish Sharma
Partner
Risk Advisory
sashish@deloitte.com

Vishal Jain
Partner
Risk Advisory
jainvishal@deloitte.com

North - Gautam Kapoor
Partner
Risk Advisory
gkapoor@deloitte.com

South - Maninder Bharadwaj
Partner
Risk Advisory
manbharadwaj@deloitte.com





Deloitte.