ANALYSIS

The Digital Personal Data Protection Act, 2023 - India's Data Protection Revamp

11 August 2023

Partners: *Rahul Matthan, Nikhil Narendran, Jyotsna Jayaram,* ***Counsels:*** *Thomas J Vallianeth, Karishma Sundara,* ***Senior Associates:*** *Akshaya Parthasarathy, Krati Hashwani,* ***Consultant:*** *Shreya Ramann,* ***Associates:*** *Akanksha Singh, Karthik Rai, Pranay Jalan, Kuruvilla M Jacob, Sidharth Ray and Sarashika Eakambaram*

Introduction

On 9 August 2023, the Rajya Sabha passed the Digital Personal Data Protection Bill, 2023. Having already been passed by the Lok Sabha on 7 August 2023, it now just needs to receive the President's assent before it becomes the Digital Personal Data Protection Act, 2023 (**DPDP Act**). Once in force, it will replace the data protection regulations contained in the Information Technology Act, 2000 to offer a comprehensive data protection regime for the country.

The Digital Personal Data Protection Bill, 2023 has been passed by Parliament, and is all set to change the data protection landscape in the country. This analysis takes a closer look at its important provisions.

Briefly, the DPDP Act:

- applies uniformly to ***all*** digital personal data irrespective of sensitivity;
- prescribes consensual and non-consensual grounds for processing personal data;
- specifies obligations for data fiduciaries (called data controllers in the European Union (**EU**));
- designates certain data fiduciaries as significant data fiduciaries (**SDF**) with additional obligations;
- sets out the rights of data principals (called data subjects in EU) and their duties;

- permits cross-border data flows but allows the government to restrict data transfers to certain geographies;
- levies penalties of up to INR 250 crore (USD 30 million) for various significant contraventions;
- establishes a Data Protection Board (**Board**) to regulate and enforce the DPDP Act's provisions with appeals lying before the Telecom Disputes Settlement and Appellate Tribunal (**Appellate Tribunal**).

While the Act does not stipulate a transitional period, the central government has been granted the discretion to notify the commencement of different provisions on different days. Until this Act is brought into force, it is likely that the corresponding provisions under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**Privacy Rules**) will continue to apply. While businesses continue to comply with the Privacy Rules in the interim period, they will also have to ensure that the provisions of the DPDP Act have been factored into their processes and technology, and that data transfers (if any) also account for requirements under the DPDP Act.

This analysis covers the key provisions of the Act and their implications. Over the course of the coming days and weeks, we will take a closer look at the implications of various newly introduced concepts and others which, although drawn from international practice, contain subtle nuances that would require data fiduciaries to consider them differently in the Indian context.

The topics covered in this update are:

1 Applicability ____ 2

2 Grounds of processing ____ 3

3 Obligations of data fiduciaries ____ 5

4 Data pertaining to certain protected classes of data principals ____ 6

5 Significant data fiduciaries ____ 7

6 Rights and duties of data principals ____ 7

7 Cross-border transfers of personal data ____ 8

8 Partial exemptions from the obligations of the Act ____ 8

9 Personal data breaches and reporting obligations ____ 9

10 Oversight ____ 10

11 Penalties ____ 10

12 Blocking directions ____ 10

13 Voluntary undertaking ____ 10

1 Applicability

- ***Geographic applicability***: The Act applies to all processing of digital personal data that occurs (a) *within India*; as well as (b) *outside India* in relation to any activity relating to the offering of goods or services to data principals in India. In the case of offshore processing, however, the text suggests that profiling that is *not* in connection with the provision of goods or services to data principals in India will not come within the ambit of the Act.

- *Personal data*: Personal data under the Act refers to data about an individual who is identifiable either by such data or in relation to such data. This suggests that anonymised data (or non-personal data) will fall outside the scope of the DPDP Act. It only applies to personal data that is collected in digital form or, if first collected in non-digital form, that has been subsequently digitised. It excludes offline (or analogue) data.
- *Automated processing*: The term *'processing'* has *wide* import under the Act. It extends to all automated (whether wholly or in part) operations performed on digital personal data, and includes the collection, recording, organisation, storage, retrieval, use, indexing, sharing, erasure and destruction of such personal data. Any *wholly* non-automated processing of personal data is excluded from the applicability of the Act.
- *Publicly available data*: The Act does not apply to personal data that has been made (or caused to be made) publicly available either (a) by the individual to whom it relates, or (b) by a third party required by law to make it publicly available. For example, if an individual maintains a public social media profile (i.e., to which access is not restricted), the Act will not apply to the processing of any personal data that has been made available on that profile.
- *Personal or domestic processing*: The Act also does not apply to processing of personal data for any personal or domestic purpose.
- *Exemptions*: The central government can exempt certain processing activities from the application of the Act:

  a. processing by government instrumentalities for specific purposes, such as in the interest of sovereignty and integrity of India, security of the State and friendly relations with foreign States; and

  b. processing that is necessary for research, archiving or statistical purposes subject to the personal data not being used for making any decision specific to a data principal, and being carried out in accordance with standards that may be prescribed by the central government.
- *Specific exemptions*: The central government may also exempt certain entities or a class of entities, such as start-ups from complying with certain provisions of the Act.

2 Grounds of processing

- *Lawful purpose*: Data fiduciaries must only process personal data for a lawful purpose and, barring limited exceptions to the rule, must do so either on the basis of consent or for certain legitimate uses.
- *Consent*: Data fiduciaries can process personal data based on consent obtained from data principals that must be:

  a. free, specific, informed, unconditional, and unambiguous;

  b. provided through clear affirmative action; and

  c. limited to the personal data that is necessary for the specified purpose.
- *Notice*: In order to obtain consent for processing, the data fiduciary must first present the data principal with a notice that specifies:

  a. what personal data is to be collected;

  b. the purposes for which such personal data will be processed (the specified purposes);

  c. how the data principal can make a complaint to the Board;

d. how the data principal can exercise their rights under the Act; and

e. the contact details of the relevant data protection officer (**DPO**) or any other person made responsible for responding to data principals' requests to exercise their rights under the Act.

- ***Languages***: Notice and consent must be provided in *clear and plain* language and data principals should have the option to access such notice in English or one of the 22 regional languages identified in the Eighth Schedule to the Constitution of India (e.g., Hindi, Punjabi, Sanskrit, and Tamil).

- ***Record-keeping***: Data fiduciaries should be able to demonstrate that the notice and consent requirements were met. This implies that all data fiduciaries will need to maintain a record of the delivery of notice and log each data principal's indication of consent.

- ***Revocation of consent***: Consent must be capable of being withdrawn as easily as it was given. Once a data principal has withdrawn consent, the data fiduciary must cease processing the personal data *within a reasonable time*, unless such processing is required or authorised under the Act or any other law. The data fiduciaries may either delete the personal data that they hold or ensure that such data is no longer in the nature of *'personal data'* (that is, anonymise it). Once consent is withdrawn, the data principal will bear the consequences of such withdrawal. For instance, if an individual withdraws consent for processing of personal data to run diagnostic tests, it may affect her ability to receive the diagnosis.

- ***Invalidity***: If the consent obtained infringes the provisions of the Act or any other law in force, it will be invalid to that extent.

- ***Personal data previously collected***: If a data principal had consented to the processing of her personal data before the Act is in effect, the data fiduciary can continue such processing until the data principal withdraws her consent. However, once the Act is effective, the data fiduciary is obliged to notify the data principal about such processing based on past consent as soon as reasonably practicable.

- ***Consent Managers***: Data principals may, if they so choose, provide, manage, review, or withdraw their consent *via* a *'consent manager'*. Consent managers provide data principals with an accessible, transparent and interoperable platform to make decisions about their consent. Every such consent manager must be registered with the Board and will be *'accountable'* to the data principal. Consent managers must provide data principals with *'readily available means'* to redress any grievances levelled at them and will be subject to penalties for non-compliance with their *'obligations'* or a breach of any registration condition. The introduction of a consent manager in the Act gives legislative support to the construct that is already operational under the Account Aggregator framework as well as the NITI Aayog's Data Empowerment and Protection Architecture.

- ***Certain legitimate uses***: The Act also permits the processing of personal data based on specific legitimate uses as an alternative to consent. This includes non-consensual grounds of processing that are commonly available in other jurisdictions, *e.g.*, processing for:

a. medical treatment;

b. health services;

c. disaster relief;

d. compliance with a judgment; and

e. responding to an emergency.

- *Voluntary provision of data*: The Act also permits the processing of personal data *voluntarily* provided by the data principal for a *specified purpose*. To rely on this ground of processing, data fiduciaries must be able to demonstrate that the personal data is only used for the specified purpose for which it was provided, and that such processing will cease once the data principal indicates that she no longer agrees to such processing. For instance, an individual who engages a shipping company to assist with relocation services may voluntarily provide her personal data (*e.g.*, contact details, and address) to the shipping company to receive these relocation services. The shipping company can only process the personal data to provide these relocation services; it cannot use it to send the individual here promotional messages unless consent is separately taken for this purpose.

- *Employment-related processing*: Another legitimate use that will have wide application, is where processing is carried out for employment purposes, or to protect employers from loss or liability. Employers handle vast amounts of personal data from the moment an employee joins the organisation (*e.g.*, bank account, Aadhaar and medical information) as well as during the course of their employment (*e.g.*, biometrics collected to register attendance or enable access control). Employers will not have to obtain express consent in order to process this personal data.

3 Obligations of data fiduciaries

Data fiduciaries are responsible for complying with the following obligations:

- *Completeness, accuracy and consistency*: They must ensure the completeness, accuracy and consistency of the personal data that they process, if it is to be:

  a. used to make a decision that affects a data principal, or

  b. disclosed to another data fiduciary.

  Data fiduciaries will need to make additional efforts to comply with this obligation, given that it can sometimes be difficult to have a '*complete*' set of all personal data, and they may not always have visibility on the corroborative personal data required to determine accuracy.

- *Notifying personal data breaches*: Data fiduciaries must notify the Board and *each affected data principal* of *every personal data breach*. In the absence of a materiality threshold for such notification, any instance falling within the definition of a personal data breach must be reported *even if it does not* involve personal data that is innately sensitive; or have a negative impact on the data principal. Data fiduciaries face penalties of up to INR 200 crore (USD 24 million) if they do not notify data principals or the Board in the prescribed manner. Notably, current cyber security laws independently require reporting of certain types of cyber security events to the Indian Computer Emergency Response Team (**CERT-In**), which will likely continue until further notice.

- *Technical safeguards and reasonable security measures*: Data fiduciaries must implement appropriate technical and organisational measures to ensure that they effectively observe the provisions of the Act (e.g., data retention standard operating procedures; a notice and consent logging mechanism); and take reasonable security measures to prevent personal data breaches (e.g., encryption, if appropriate). The breadth of these terms suggests that data fiduciaries have some latitude in determining what the *'appropriate'* measures or safeguards would be in such instances. A failure to take reasonable security safeguards to prevent personal data breaches carries with it a penalty of up to INR 250 crore (USD 30 million).

- ***Prohibition on retention of personal data***: Data fiduciaries are obliged to *erase personal data* when a data principal withdraws consent, or as soon as it is reasonable to assume that the specified purpose for collection of personal data is no longer served by its retention. The Act suggests that a specified purpose is no longer served where a data principal does not, for a prescribed time period, approach the data fiduciary for the performance of the specified purpose *and* exercise her rights in relation to such processing. Different periods of time may be prescribed for different classes of data fiduciaries and for different purposes.
- ***Details of a grievance officer***: Data fiduciaries must publish the business contact information of a person who may answer a data principal's queries pertaining to the processing of their personal data (such as a DPO where the data fiduciary qualifies as an SDF).

Data fiduciaries cannot justify non-compliance with their obligations under the Act based on a data principal's failure to carry out her (corresponding) duties. They also cannot contract out of their obligation to process personal data in consonance with the Act. For example, even if a data fiduciary requires a data processor to undertake reasonable security safeguards under a contract, it does not absolve the data fiduciary of its obligation to ensure that such reasonable safeguards were, in fact, undertaken or the imposition of a penalty on the data fiduciary (if the Board determines this applies).

4 Data pertaining to certain protected classes of data principals

Processing the personal data of children and disabled persons with guardians carries additional obligations under the Act. The Act defines a child as an individual under the age of 18 but does not similarly define *'a person with disability'*. However, a reference may be made to the Rights of Persons with Disabilities Act, 2016, which contains a definition of this term.

The following provisions would need to be kept in mind when processing personal data of such protected classes of data principals:

- ***Verifiable consent***: Data fiduciaries must, prior to the processing of the personal data of children or persons with disability who have a legal guardian, obtain verifiable consent of a parent or legal guardian, as applicable. The process for obtaining such verifiable consent is yet to be prescribed.
- ***Prohibition on processing, tracking, and behaviour monitoring***: Data fiduciaries are prohibited from undertaking any processing that is likely to have a detrimental effect on the well-being of a child and tracking, monitoring the behaviour of, or directing targeted advertisements at children. The data fiduciary cannot overcome these prohibitions by obtaining parental consent. Data fiduciaries may need to revise their existing systems to ensure that they are in compliance with these requirements.
- ***Exemptions while processing children's data***: The central government has the power to exempt data fiduciaries from the obligation to obtain verifiable parental consent and the prohibitions on tracking, behavioural monitoring and targeting advertisements at children in the following circumstances:

  a. for prescribed purposes, or for certain data fiduciaries or classes of data fiduciaries; or

  b. for processing personal data of a child above a particular age that is to be prescribed, if carried out by certain data fiduciaries who satisfy the central government of their verifiably safe processing of children's data.

Neither of these exemptions is available for processing the personal data of a disabled person with a guardian.

5 Significant data fiduciaries

In addition to the obligations prescribed for data fiduciaries, the Act prescribes some additional obligations for *'significant data fiduciaries'*. SDFs will be separately notified by the central government based on factors such as the volume and sensitivity of personal data processed, the risk posed to the rights of the Data Principal, the potential impact on the sovereignty and integrity of India, the risk to electoral democracy, security of the State, and public order. For instance, payment applications processing a high volume of payments or telecom service providers may be classified as SDFs on the basis of a combination of such factors (e.g., volume and sensitivity of personal data processed as well as the risk to the rights of a data principal), or based on a single, standalone factor (e.g., risk to the rights of a data principal). Once notified as SDFs, these entities will have the following additional obligations:

- *Appointing a Data Protection Officer*: SDFs must appoint a DPO based in India to act as their representative for the provisions of the Act and as the single point of contact for grievance redressal. This DPO must be an individual who is responsible to the board of directors or similar governing body of the SDFs. The Act does not prescribe any other qualifying criteria for a DPO.
- *Appointment of an independent data auditor*: An SDF must appoint an independent data auditor to evaluate the SDF's compliance with the Act. The Act does not, however, specify the periodicity for conducting such audits, or the technical or operational qualifying criteria for auditors.
- *Other measures*: SDFs must also undertake data protection impact assessments (DPIA), periodic audits, or other measures that may be prescribed by the central government. The Act clarifies that the DPIA refers to a process that comprises a description of the rights of data principals, the purpose of processing their personal data, an assessment and management of risks to their rights, and such other matters with respect to the processing of personal data which the central government may prescribe.

6 Rights and duties of data principals

Data principals have certain rights with respect to their personal data. All these rights, discussed below, can be exercised against data fiduciaries, but only one of them (the right to grievance redressal) is also available to data principals in the context of consent managers, where such consent managers are not data fiduciaries.

- *Right to access*: The Act grants data principals the right to request and obtain a summary of personal data being processed, and processing activities undertaken in this respect, the identities of all data fiduciaries and data processors with whom their personal data has been shared, and any other information related to the personal data or its processing, as may be prescribed. The request must be made by the data principal in the manner prescribed by the central government. Save for certain exceptions (such as where personal data has been shared with another data fiduciary for the investigation of offences), there is no scope to refuse requests in the exercise of this right. Data fiduciaries must mandatorily honour such requests.
- *Right to correction and erasure*: Data principals can request a data fiduciary to correct, complete, or update their personal data. They also have the right to seek the erasure of their personal data in a form that may be prescribed by the central government. Data fiduciaries are required to act on such request unless this personal data is necessary for the specified purpose or is necessary for compliance with laws in force.

The right to access, and the right to correction and erasure are only applicable in relation to personal data where it is processed based on consent or on the basis of the *voluntary legitimate use* ground. In other words, these rights are not available where a data principal's personal data has been processed on the basis of any other legitimate use specified under the Act (such as for employment purposes).

- *Right to nominate*: Data principals have the right to nominate an individual to exercise their rights in the event of their death or incapacity.
- *Right of grievance redressal*: Data fiduciaries and consent managers must provide data principals a readily available means of grievance redressal for any matters pertaining to this Act. While no specific period would need to be adhered to until prescribed, data fiduciaries and consent managers may need to be prepared to create such systems and form standard operating procedures to provide redressal measures.
- *Duties of data principals*: The Act also imposes certain duties on data principals. These include the duty not to impersonate another person, and to provide only such information as may be verifiably authentic when exercising their right to correction or erasure. Their failure to do so may carry a penalty of up to INR 10,000 (USD 120). The fact that a data principal has not complied with its duties will not be a justification for a data fiduciary to not comply with its own obligations.

7 Cross-border transfers of personal data

The Act does not restrict data fiduciaries from transferring personal data to other countries. However, it permits the central government to specify certain territories or geographies to which the transfer of personal data may be restricted. The central government is expected to publish a blacklist of countries/territories in this regard. It is likely that such a list will only include nations that India regards as unfriendly.

The wording of the provision is broad, leaving room for the central government to use this notification to impose additional conditions on such cross-border transfers. It is, thus, presently unclear whether additional conditions for a transfer to a specific country could be imposed through delegated legislation as opposed to an absolute restriction on transfer to a notified country. Further, the question of what constitutes *'transfer'* for the purposes of this provision is still unclear. For instance, the Act does not clarify whether personal data collected by a foreign data fiduciary or data processor directly from Indian residents would be considered a *'transfer'*.

The Act, however, does not prevent any other law from prescribing a higher threshold of data protection, such as the data localisation requirements that have been imposed in relation to payments data or telecom data.

8 Partial exemptions from the obligations of the Act

- *Exemptions for specific processing activities*: Certain processing activities may be exempted under the Act in each of the following cases:

  a. processing by legal authorities performing judicial, regulatory or supervisory functions;
  b. processing for the prevention, detection, investigation or prosecution of any offences; to determine the financial position of any person who has defaulted on an institutional loan or advance; in relation to authorised mergers and acquisitions; and for enforcing a legal right; and
  c. processing personal data of data principals outside of India pursuant to a contract with a foreign party.

Personal data processed in these cases does not require notice or a legal basis for processing. Barring the requirement to implement reasonable security safeguards to protect personal data, it is not subject to any data fiduciary obligations, including those in relation to SDFs or protected classes of data principals; and will not be subject to any data principal rights or duties.

- *Exemptions based on volume and nature of personal data*: The central government has the power to exempt certain data fiduciaries, or classes of data fiduciaries, from various provisions of the Act based on the volume and nature of data they process. Entities that process low volumes or low-risk data, such as small businesses or start-ups, may be covered within this exemption. If exempted, such entities would not be required to provide a notice prior to collecting consent; ensure completeness, accuracy, or consistency of the personal data; erase personal data upon request or when the specific purpose is served; undertake any obligations as an SDF; or provide data principals with the right to access their personal data.
- *Exemptions for the State*: Every State body or agency is permitted to process data without ensuring completeness, accuracy or consistency of the personal data; is not obliged to erase data upon request; and is not required to offer for it to be corrected, made complete or updated upon request, provided that this data is not being processed to make a decision that may affect the relevant data principal.
- *Residual power of exemption*: The central government can, if it is so inclined, notify any data fiduciary or class of data fiduciaries as being exempt from any of the provisions of the Act for a specified time period.

9 Personal data breaches and reporting obligations

The term '*personal data breach*' is defined broadly to include any unauthorised processing of personal data, accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to personal data that compromises the confidentiality, integrity, or availability of such data.

- *Reporting of personal data breaches*: If a personal data breach occurs, data fiduciaries must promptly inform each affected data principal and the Board of such a breach. Given the broad definition, there will be a reporting requirement even for minor contraventions of the provisions of the Act itself (such as where processing has been undertaken without consent or legitimate use). No timeline has been prescribed for reporting personal data breaches. The specific format and method of reporting are yet to be prescribed under the Act. Upon receiving intimation of a breach from a data fiduciary, the Board may direct the data fiduciary to undertake urgent remedial or mitigation measures to minimise the impact of the breach. Additionally, the Board may investigate a personal data breach and levy penalties based on either an intimation received from the data fiduciary or a complaint lodged by the data principal. No materiality thresholds have been established for the reporting requirement. As a result, data fiduciaries would have to comply with these obligations for all types of personal data breaches, regardless of the sensitivity of the breach or its impact on the data principal.
- *Regulatory overlaps*: The Act is not alone in imposing a reporting obligation for data breaches. The existing cyber security framework already requires certain types of cyber security events (including data breaches) to be reported to CERT-In. In the absence of information to the contrary, both regimes will apply. Data fiduciaries will need to reassess their practices and procedures related to breach reporting and evaluate each instance against the guidance provided under this law, as well as the cyber security laws, to determine if it qualifies for reporting under either regime. Data fiduciaries must deploy appropriate organisational capabilities to identify and report cybersecurity incidents within the applicable timelines.

10 Oversight

The Board will oversee the implementation of the Act. Data principals may report contraventions of the Act to the Board. These contraventions may also be referred to the Board by the central government or a court. Where there are sufficient grounds to scrutinise a contravention, the Board will conduct an inquiry and communicate its decision in writing. Alternatively, the Board may, in some instances, refer the complainant and contravening party to mediation. A determination of the Board may be appealed before the Appellate Tribunal, whose decision may, in turn, be appealed before the Supreme Court, if there is a substantial question of law involved. Civil courts cannot entertain suits or take action under the Act, although certain remedies, such as writs (where applicable) cannot be precluded.

11 Penalties

Substantial monetary penalties of up to INR 250 crore (USD 30 million) have been prescribed for various significant contraventions. While not maintaining adequate security safeguards could attract the highest penalty, non-compliances with other obligations relating to children and personal data breach reporting may result in penalties of up to INR 200 crore (USD 24 million). SDFs may also be fined up to INR 150 crore (USD 18 million) for not meeting the additional obligations imposed on them. A general residuary penalty of up to INR 50 crore (USD 6 million) has also been prescribed for a breach of any other provision of the Act or any rule issued under it.

While the Act does not prescribe the parameters that would inform the Board's determination on significance, the Board, in arriving at the quantum of the penalties, may consider a number of factors such as the nature, gravity and duration of the contravention, types of personal data affected, implications of the contravention and mitigating measures adopted by the contravening party.

As the penalties payable under the Act are not subject to a ceiling, multiple contraventions could carry a significantly hefty penalty. There is no clarity on whether multiple contraventions of the same provision, or contraventions in relation to multiple data subjects, will enhance the penalty imposed. The central government can also increase these penalties, although the elevated sum cannot surpass twice the numbers presently prescribed.

12 Blocking directions

The Act also permits the central government, in the interest of the general public, to order intermediaries (like cloud service providers or internet service providers) to block access to information contained in any computer resource that enables a data fiduciary to provide goods or services to data principals in India, where the data fiduciary is a repeat offender that has been subject to a monetary penalty at least twice. If the intermediary fails to comply, it can also be subject to a fine of up to INR 50 Crore (USD 6 million).

13 Voluntary undertaking

The Act encourages contravening parties to, at any stage of a proceeding before the Board, voluntarily admit non-compliance and undertake to adopt rectification measures. Once the voluntary undertaking is accepted by the Board, the contravening party is immune from any further proceedings based on the terms of the undertaking, although the Board may vary these terms with the party's consent. That said, if the terms of the voluntary undertaking are not complied with, the penalty applicable to the underlying contravention may be imposed on the contravening party.

Conclusion

The Act ushers in a new phase of technology law in India. With most of the substantive compliance obligations carved out under the Act hinging on delegated legislation, compliance with the law will have to evolve alongside it.

While some obligations applicable to data fiduciaries may impose a heavier, operational burden in the short run (e.g., providing data principals the option to access notice-consent flow in Indian languages), the bulk of the obligations empower the data fiduciaries to apply steps suited to them, provided the objective is achieved (e.g., implementing reasonable security safeguards to prevent a data breach). By creating exclusions to its applicability (e.g., placing non-digital data or non-personal data outside its scope) and leaving room for exemptions in specific circumstances, the Act provides scope for some deliberation.

All members of this new ecosystem - data fiduciaries, processors and data principals - have a long, but insight-filled road ahead of them, as they acclimatize to its requirements, shortcomings and benefits.
