DPDPA Incident Response Process Considerations and Template Policy – May 2026

This paper analyzes the requirements for personal data breach notification under India's Digital Personal Data Protection Act, 2023[1] (the DPDPA) and provides a discussion draft template policy for assessing privacy and security incidents to determine if they trigger these notification requirements.

Background:

Under the DPDPA, data fiduciaries are obligated to provide notice of any "personal data breach" to the Data Protection Board of India and to each affected data principal. [Chapter 2, 8(6)]

The DPDPA defines a "**personal data breach**" as:

> any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data. [Chapter 1, 2(u)]

The Digital Personal Data Protection Rules, 2025[2] prescribe the form and manner of the notifications. Rule 7 states:

(1) On becoming aware of any personal data breach, the Data Fiduciary shall, to the best of its knowledge, intimate to each affected Data Principal, in a concise, clear and plain manner and without delay, through her user account or any mode of communication registered by her with the Data Fiduciary, —
   (a) a description of the breach, including its nature, extent and the timing of its occurrence;
   (b) the consequences relevant to her, that are likely to arise from the breach;
   (c) the measures implemented and being implemented by the Data Fiduciary, if any, to mitigate risk;
   (d) the safety measures that she may take to protect her interests; and
   (e) business contact information of a person who is able to respond on behalf of the Data Fiduciary, to queries, if any, of the Data Principal.

(2) On becoming aware of any personal data breach, the Data Fiduciary shall intimate to the Board, —
   (a) without delay, a description of the breach, including its nature, extent, timing and location of occurrence and the likely impact;
   (b) within seventy-two hours of becoming aware of the breach, or within such longer period as the Board may allow on a request made in writing in this behalf, —
      (i) updated and detailed information in respect of such description;
      (ii) the broad facts related to the events, circumstances and reasons leading to the breach;
      (iii) measures implemented or proposed, if any, to mitigate risk;
      (iv) any findings regarding the person who caused the breach;
      (v) remedial measures taken to prevent recurrence of such breach; and
      (vi) a report regarding the intimations given to affected Data Principals.

The DPDPA differs from GDPR and most US state breach notification laws in that it does not provide an exception for breaches that are low risk or that do not involve sensitive data elements. For example, GDPR Article 33 provides that regulatory notification is not required if the breach is "unlikely to result in a risk to the rights and freedoms of natural persons." US state laws, such as California's breach notification law,[3] are only triggered if the impacted information

[1] https://dpdpa.com/DPDPA_2023_official.pdf

[2] https://dpdpa.com/DPDP_Rules_2025_English_only.pdf

[3] California Civ. Code s. 1798.82(a)

includes sensitive data elements, such as a person's Social Security number, other government-issued identification numbers, financial or medical data or similar information that, by its nature, puts an individual at risk if exposed.

While these explicit exceptions for low risk breaches allow companies to build sensible filters into their notification processes, the lack of such an exception does not mean that all privacy events must be notified in India. It is critical that we establish rules to determine *when* an incident becomes a personal data breach and *how* to fulfill the reporting requirements in an effective, efficient manner.

Determining Whether a Personal Data Breach has Occurred

As noted above, a "personal data breach" occurs when a data fiduciary subject to the DPDPA experiences either:

(1) the *unauthorised processing* of personal data, or
(2) the a*ccidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access* to personal data, that *compromises the confidentiality, integrity or availability* of the personal data.

If either of these has occurred, the event is a reportable personal data breach under the Act and Rule 7.

We can consider each of these triggers separately.

Breaches Caused by Unauthorized Processing

In some cases, it will be clear that unauthorized processing of personal data has created a personal data breach. For example, if a company discovers that a rogue employee is using customer account data to impersonate the customers and commit fraud, the company clearly has an obligation to report this incident under the DPDPA.

In other cases, however, the company may receive a complaint regarding unauthorized processing which needs to be evaluated to determine if a breach has occurred. The DPDPA's reliance on consent as the primary legal basis for processing creates an environment where questions about authorization are likely to arise. For example, an employee may express a concern that a particular processing activity is unauthorized because they do not believe that the data principals have consented. A data principal may file a grievance that their data have been processed outside the scope of their consent. Are these personal data breaches? The company must consider risks of un- and under-permissioned processing in the incident response process.

If the privacy office can establish that the processing is justified based on a DPDPA legal basis, there will be no breach. Possible legal bases include (from the DPDPA Chapter II, 7): compliance with law, court orders and judgements; protecting the vital interests of the principals in the case of medical emergencies, public health, disasters; and employment purposes (for true employees). Processing can also be justified based on DPDPA Chapter IV, 17(1), which authorizes processing for a variety of other purposes, including enforcing legal rights; preventing, detecting, investigating and prosecuting crimes; M&A transactions; payment defaults; and certain types of State-sponsored research (pursuant to the Second Schedule).

Similarly, if the privacy office can establish that the processing either (1) involves personal data collected directly from the data principal for purposes specified at the time, or (2) is within the scope of the consent obtained from the data principal, there is no issue. (Chapter II, 4.)

Unfortunately, we can anticipate that the privacy office may be asked to determine if processing is authorized in connection with a specified purpose or by a consent document, when the scope of the permissioned use is less clear. To aid this determination, we should establish some objective standards to use when evaluating the appropriateness of a secondary processing activity in the context of a specified purpose or a consent form.

Prior to GDPR's codification of legitimate interest as a legal basis for processing, we relied on contractual necessity and consent to process EEA data. Historically, we understood that processing permitted by these legal bases extended to allow processing for secondary purposes if they were "compatible" or "closely related." Customary internal business purposes were encompassed by this standard. (If I consented to receive marketing communications,

it was understood that I also consented to traditional CRM activities and other types of processing, such as the duplication of my data in back-ups.) Much was written about the types of secondary processing that could be bundled, but the concept of compatible purposes was firmly established for those types of ancillary processing activities that were reasonably expected by data subjects and regulators. In other words, compatible processing activities can be appropriate, depending on the nature of the proposed processing *and* whether the proposed processing is reasonably expected by the individual.[4]

Similarly, the California Consumer Privacy Act restricts the purposes for which personal information can be processed, to those disclosed purposes that are "reasonably necessary and proportionate" to achieve either the purposes for which it was collected or for other disclosed *compatible* purposes.[5] The CCPA regulations clarify that these purposes must also be consistent with an individual's reasonable expectations. Section 7002(c) of the regulations provides that whether another disclosed purpose is compatible will depend on: (1) the reasonable expectations of the consumer, (2) the nature of the other processing purposes, and (3) the strength of the link between the purposes.[6]

This concept of compatible purposes is useful when assessing processing activities under the DPDPA. It will never be possible to obtain explicit consent for every type of processing activity that a company may engage in; we must assume that related processing activities can be bundled if compatible. If we are processing data to provide a product, we should be able to assume that we can process the data in the event of a product recall. However, any authorization can only be valid for those processing activities that are reasonably expected; as a foundational matter, people cannot consent to processing that is truly unexpected. The question then becomes, what do people expect?

While the DPDPA does not recognize legitimate interest as a legal basis, the GDPR does. However, to rely on legitimate interest, companies must document that the processing is reasonably expected; this is a foundational requirement under GDPR.[7] In December 2016, the Conference Board published a white paper entitled *Data Processing Based on Legitimate Interests*[8] that explored the types of compatible processing activities that should be "reasonably expected." Annex 1 to this paper includes a comprehensive inventory of the types of processing activities that should generally be expected, given the context. This work provides a useful starting point for our assessment of the scope of any given DPDPA authorization.

When analyzing whether a secondary processing activity can be undertaken under the DPDPA based on its compatibility with an authorized processing activity, the company should ask three questions:

- Is the secondary processing activity itself specified or described in the notice accompanying the consent form? *If so, the processing is authorized*.

- If not, should the processing be expected given the language in the consent and/or the nature of the processing that was authorized? *If not, the processing is unauthorized*.

- Are there other factors that make the processing incompatible with the consent? *For example, the company might have told the principal that it would not process the personal data in a particular way. Or the processing could have a disproportionately adverse impact on the individual*. These factors would lead the privacy office to conclude that the processing is not authorized.

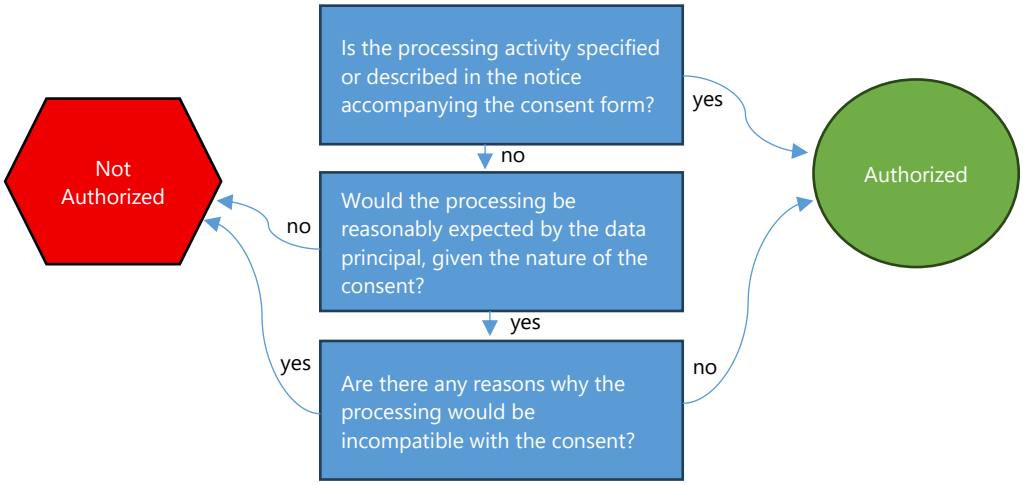
[4] To the extent the processing is not reasonably expected, it will almost never be deemed compatible.

[5] Cal Civ Code §1798.100(c)

[6] 11 CCR §7002. Per §7002(c)(3): "For example, a strong link exists between the consumer's reasonable expectations that the personal information will be used to provide them with a requested service at the time of collection, and the use of the information to repair errors that impair the intended functionality of that requested service. This would weigh in favor of compatibility. By contrast, for example, a weak link exists between the consumer's reasonable expectations that the personal information will be collected to provide a requested cloud storage service at the time of collection, and the use of the information to research and develop an unrelated facial recognition service."

[7] See, *e.g.,* GDPR Recital 47

[8] https://www.conference-board.org/publications/Data-Processing-Based-on-Legitimate-Interests



Examples can help illustrate how these questions would be applied in practice.

- Consider a visitor to a company's facility: she consents to the collection of her name and contact information in the visitor log, pursuant to a notice that says the personal data will be used to create a guest pass, record her visit, and for health and safety purposes. However, during her visit a theft is reported. The visitor is not suspected of being involved with the theft, but the company would like to use her contact details to request an interview as part of their investigation. *Is this processing authorized?* Yes. The visitor should expect that her data would be processed in connection with physical security matters generally. The company could also disclose her contact details to their own private investigators or to local law enforcement officers so that they could ask if she observed anything relevant to the investigation. *These are all authorized processing activities.* The company should take care, however, that it does not suggest she was involved in the theft; that would be unexpected and detrimental to the visitor's reputation.

- Consider a customer who contacts a company about a problem she is having with the company's product. The company representative tells the customer that he needs to look up her account information to learn what product model the customer has purchased, and the customer agrees. After the call, the company sends a satisfaction survey to the consumer to learn her views of its support function. The customer alleges that the survey is unauthorized, as she did not consent to her personal data being processed to send a survey. The customer service function asks whether sending surveys represents a personal data breach under the DPDPA. *Is this processing authorized?* While the better practice would be to obtain consent specifically to send the follow-up survey, the processing of the customer's personal data to send the survey was not unauthorized for personal data breach analysis. The customer consented to the processing of her data in connection with her service request, and it was reasonable for the company to send a survey to confirm that her request had been properly handled. The processing would have been unauthorized if the customer had specifically indicated that she did not consent to receiving a follow-up communication, or if the representative had explicitly told her that she would not be contacted.

  Note that the compatibility test here also hinges on the survey being tied to the support request. If the company wanted to send a marketing communication to people who contacted the service desk, it would have to obtain consent. The secondary processing for marketing cannot be considered compatible; nor is likely expected by the consumer.

Note that the process has implications far beyond the company's incident response program. When a company evaluates new processing activities in the context of its PIA program, this same standard can help a company determine if previously collected data can be used or if an additional consent pass is needed.

Breaches Caused by Accidents that Compromise the Personal Data

The breach notification rule is also triggered by a*ccidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access* to personal data, that *compromises the confidentiality, integrity or availability* of the personal data. This provision is where companies will feel the lack of a risk of harm exception most keenly. However, it is important to note that the breach notification rule is not triggered by any accidental disclosure (*etc.*) *per se*, only by those accidents that compromise the confidentiality, integrity or availability of the data.

While many US laws use the word "compromise" in their definition of breach,[9] the word is not itself defined in the laws. This means we should look to the plain meaning of the word to understand it. In the context of a security breach, "compromise" must be read as "cause the impairment of" or "expose to an unauthorized person, especially an enemy."[10] If we haven't impaired the data or exposed it to someone who could be a threat actor, it has not been compromised.

We see this view in the US laws. The vast majority of the US state breach notification laws follow California and explicitly state that "good faith acquisition of personal information by an employee or agent of the individual or business for the purposes of the individual or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure," reflecting that these types of incidents do not compromise the personal data.

The DPDPA "compromise" standard is in fact almost identical to the breach notification standard under the US Federal Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule.[11] Under HIPAA, privacy and security obligations apply to "protected health information" (PHI), which is broadly defined as any individually identifiable data maintained by an entity subject to the HIPAA rules. These entities must provide notice of any "breach" without regard to specific data elements and without any risk of harm exceptions; "breach" is defined as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [HIPAA] which compromises the security or privacy of the protected health information."

The US Department of Health & Human Services has provided substantial guidance on the application of the HIPAA Breach Notification Rule. For example, following the US state approach, "breach" does not include any good faith unintentional acquisition, access, or use of PHI by an entity's workforce member, agent or service provider or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use does not result in further unauthorized use or disclosure. It goes farther, adding that a disclosure of PHI is not a breach where the company (or its processor) has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

The HIPAA Rule provides that any other acquisition, access, use, or disclosure of protected health information is presumed to be a breach unless the entity "demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment addressing the following factors:

(i) The nature and extent of the information involved, including the types of identifiers and the likelihood of re-identification,

(ii) The unauthorized person who used the information or to whom the disclosure was made,

(iii) Whether the information was actually acquired or viewed, and

(iv) The extent to which the risk to the information has been mitigated.

[9] *E.g.*, the California statute cited above defines "breach of the security of the system" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of [the] personal information..."

[10] https://www.merriam-webster.com/dictionary/compromise

[11] Notification in the Case of Breach of Unsecured Protected Health Information, 45 CFR Part 164 Subpart D

This 4-factor test to determine if the information has been compromised is very valuable, as it provides an objective standard and enables consistency in conducting breach investigations. In particular, use of these factors makes it clear that the acquisition of unencrypted sensitive personal data by an untrusted recipient creates a high risk of harm; while also allowing companies to demonstrate that personal data may not have been compromised, even if sensitive personal information is exposed, if the recipient is trusted, the data is recovered, and any residual harm is mitigated.

As a practical matter, much attention is spent on documenting the types of incidents that put individuals at risk of harm, but many incidents do not compromise the personal data. For example, many companies have invested heavily in encryption technology, precisely to ensure that data are not compromised if they are exposed. The loss of encrypted personal data should not be viewed as a personal data breach, so long as the encryption keys themselves are not compromised. Ensuring that companies who use strong encryption have a path to avoid costly breach notification will encourage even greater deployment of that technology.

Similarly, companies and regulators need to focus on managing incidents where personal data are compromised, and where steps need to be taken to mitigate possible harm. Over-notification (particularly where there is no real risk to mitigate) can create notification fatigue and reduce the likelihood that individuals will act on a notification letter, even when action is needed.

Attachment 1 below contains a discussion draft template incident response policy that may be tailored to address DPDPA breach notification requirements, incorporating a scorecard (based on the US Health & Human Services model) to assess whether personal data have been compromised. The policy follows the industry best practice of a three-step approach to privacy breaches:

1st Are individuals at real risk of harm? If so, notify the individuals as soon as possible, and (to the extent possible) mitigate the risk. Notify regulators and others (such as law enforcement agencies, payment card fraud teams, *etc.*) as appropriate or necessary. *If there is real risk, individuals should be notified even if there is no legal obligation to do so.*

2nd Is there a legal obligation to notify? If individuals are not at real risk of harm, provide notifications as may be required by law, such as if there is unauthorized processing or if the data have been compromised, triggering the DPDPA's breach notification requirements.

3rd If there is no risk of harm and no legal obligation to notify, document the findings and implement any organizational learning needed to reduce the likelihood of this type of incident recurring.

This template is tailored for India but follows the general form of prior PIMS incident response policy templates to enable companies to easily integrate it into their existing incident response processes. It should provide companies and regulators with a foundation from which to evaluate and standardize incident response program expectations both for India and in the wider global context.

Attachment 1 – Template DPDPA Incident Response Policy
Draft for Discussion and Consultation with Competent Indian Counsel[12]

[Company Name] ("Acme") is fully committed to protecting the security and confidentiality of all the personal information that is entrusted to us. As part of this commitment, Acme has adopted this incident response policy to guide our internal handling of incidents that may impact **personal data**, which is any data about an individual who is identifiable by or in relation to such data, subject to India's Digital Personal Data Protection Act (the DPDPA).

Acme defines a **privacy incident** as *any* occurrence that *could* compromise the privacy, confidentiality, security or integrity of personal data. Privacy incidents include any deviation from Acme's privacy or security policies, loss of Personal Data as well as any unauthorized use or disclosure of Personal Data.

Examples of privacy incidents:

- System disruption causing loss of personal data or loss of access to personal data
- Lost or stolen device containing personal data
- Misdirected package, email or fax containing personal data
- Presence of malware on a computer or device containing personal data
- Transmission of personal data other than as permitted by company policy

Acme requires all employees and contractors to report privacy incidents via an established process. We investigate all privacy incidents, to determine what happened, establish if any personal data was compromised, and (if so) evaluate the risk of harm that could result from the situation and our legal obligations to report the incident.

In many cases privacy incidents do not actually expose any personal data. For example, personal data on a lost laptop may have been strongly encrypted so that it cannot be accessed by any unauthorized person. These data have not been compromised.

In some cases, privacy incidents do impact personal data. For example, a lost device may contain unencrypted information, or an employee may accidentally transmit a file containing personal data to the wrong recipient. These events may be personal data breaches under the DPDPA. A **personal data breach** means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.

In responding to privacy incidents impacting personal data subject to the DPDPA, it is essential that we quickly and accurately assess the event to determine if we have experienced a personal data breach. If so, we need to comply with the reporting requirements in the law.

All privacy incidents are evaluated using the following 3 step process to determine the proper company response.[13]

STEP 1: **Determine if there is a real risk of harm to the impacted individuals because of the incident.**

If so, notify individuals via their established user accounts or using any other mode of communication that may be appropriate without delay. Provide an initial notification to the Board without delay, followed by the secondary notification within 72 hours. *See DPDPA Rule 7 for the contents of these notices and additional requirements.*

[12] ***This template offers an appropriate that has not been vetted with the Indian Data Protection Board and that may not be acceptable to the Board.***

[13] This process describes the steps required to manage privacy incidents where Acme is the data fiduciary. If Acme is a data processor, it must notify the data fiduciary as soon as possible to enable its customer to address the requirements of the Act.

A privacy incident presents a real risk of harm to an individual when it is likely to have a significant detrimental effect on the individual. Incidents that could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage all create a real risk of harm. Note that harm may exist even if the personal data are not disclosed to an unauthorized entity; even a non-malicious system disruption that causes the deletion of important personal data or that prevents individuals from accessing their financial or medical records could present a real risk of harm to the individuals.

Risk must be assessed on a case by case basis, considering the circumstance of the incident and the nature of the personal data involved. For example, if sensitive data elements are exposed, such as bank account details that could put someone at risk of financial crime, risk is highly likely. Even less sensitive data elements, such as email addresses, may present a real risk of harm, if the incident puts the individual at risk of phishing. On the other hand, the loss of a staff directory containing the types of data elements found on employee business cards would not normally present a risk of harm. Similarly, if the personal data are strongly encrypted, and the encryption keys are not compromised, there is no real risk of harm.

As a matter of policy, we assume that a risk of harm exists if unencrypted personal data are stolen. We also assume that a risk of harm exists if sensitive personal data (such as national identification numbers, tax identification numbers or financial account information) has been transmitted to an unknown or untrusted recipient, even if by accident.

If there is a real risk of harm, we must notify the impacted individuals and the Data Protection Board of India without delay. The notification must include information on what steps the company is taking to mitigate the risk of harm along with information on the steps (if any) that the individuals should take. The notification must include other information required to be provided by Rule 7. *Time is of the essence.*

If there does not appear to be a real risk of harm move to step 2.

STEP 2: **Determine if there is other unauthorized processing or if there has been any accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of the personal data.**

If so, notify individuals via their established user accounts or using any other mode of communication that may be appropriate without delay. Provide an initial notification to the Board without delay, followed by the secondary notification within 72 hours. *See DPDPA Rule 7 for the contents of these notices and additional requirements.*

The DPDPA requires us to notify the Board and the impacted individuals of any unauthorized processing or if personal data have been compromised, even if there is a low risk of harm. The Incident Response Scorecard attached below is used to determine if notification is required. If the processing is unauthorized *or* if the score generated by the Incident Response Scorecard is 5 or more, notification may be required. The privacy office or legal counsel should assess the incident to determine if notification is required. If so, follow the notification procedures outlined in step 1 above.

If the score generated is 4 or less, the processing was authorized and the personal data have not been compromised. Move to step 3.

STEP 3: **Determine if any actions should be taken internally to address any weaknesses that may have triggered the investigation. Document these findings with the investigation materials and maintain documentation in accordance with Acme's document retention policy.**

When individual notifications are not required either to alert individuals to a real risk of harm or to comply with a legal notification requirement, Acme will not notify individuals of the incident.

Acme strives to learn from its investigations into privacy incidents, even when a personal data breach has not occurred. For example, if the investigation stemmed from an allegation that processing was not authorized, we should consider if the notice and consent forms should be updated for clarity. Similarly, if the investigation stemmed from the accidental disclosure of personal data to the wrong vendor, we should consider if additional training needs to be provided to the workers who are handling the files. Any recommendations should be noted and tracked to completion in the company [governance risk and compliance system].

Acme retains records of all privacy incident investigations for a minimum of five (5) years. Send copies of your documentation (including the completed Incident Response Scorecard and any notification materials) [to where] for retention.

Personal Data Breach Assessment Scorecard

Acme evaluates all privacy incidents to determine if a personal data breach that requires legal notification has occurred. A personal data breach exists if there has been any (1) unauthorised processing of personal data or (2) accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data. For purposes of this analysis, **personal data** means any data about an individual who is identifiable by or in relation to such data, and subject to India's Digital Personal Data Protection Act (the DPDPA)

(1) Determine whether the processing of the personal data was authorized.

The processing was authorized by the DPDPA for the following purpose:

- ☐ To comply with law, or to comply with a court order or judgement
- ☐ To protect the vital interests of the individual (medical emergency, public health, disaster)
- ☐ For employment purposes (for personal data pertaining to true employees)
- ☐ To enforce a legal right or claim, or to prevent, detect, investigate or prosecute any violation of law
- ☐ The processing entails non-Indian data being processed pursuant to a contract
- ☐ In connection with an M&A transaction
- ☐ In connection with payment defaults
- ☐ In connection with certain State-sponsored research (pursuant to the Second Schedule)
- ☐ Data was collected from the individual and used for the purpose specified at the time
- ☐ Consent of the data subject

Describe the circumstances and/or the consent process:

_____

_____

If the processing is not authorized, this may be a personal data breach. Consult with legal counsel.

(2) Determine if the personal data have been compromised.

Using the scorecard below, determine the likelihood that the personal data are compromised:

1. The nature and extent of the personal data involved, including the types of identifiers and the likelihood of re-identification:

For this factor, it is appropriate to consider the sensitivity of the personal data. While the DPDPA does not contain a definition of sensitive personal data, rules under India's Information Technology Act, 2000[14] recognize the following data elements as sensitive personal data: (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; and (vi) biometric information.

0 Points	1 Point	2 Points
Personal data (but no sensitive personal data) consisting of public or publicly available data, *e.g.,* business contact information. Personal data not associated with an identifiable individual, *e.g.,* data are deidentified or pseudonymized and unlikely to be reidentified.	Unencrypted, identifiable personal data (but no sensitive personal data), *e.g.,* individual names associated and email address or telephone number, purchase history, employment details or salary information.	Unencrypted, identifiable sensitive personal data De-identified personal data that could be reidentified to reveal sensitive personal data.

[14] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)

0 Points	1 Point	2 Points
Any personal data (including sensitive personal data) if encrypted using an industry standard encryption provided that the encryption keys are not compromised.	De-identifiable personal data (but no sensitive personal data) that could be reidentified.	

THIS EVENT: Circle Rating Points: 0 1 2

EXPLAIN:_____

_____

If the data are appropriately encrypted, the data are likely not compromised. Document:
(1) Encryption standard used: _____
(2) Confirm "default" key was changed:_____
(3) Confirm keys not compromised:_____
(4) Confirm that encryption was effective (e.g., device was not in "sleep mode" or other unencrypted state):_____

2. The unauthorized person who used the personal data or to whom the disclosure was made:

0 Points	1 Point	2 Points
Trusted Recipient - Acme Affiliate - Entity subject to a legal or contractual duty of confidentiality to Acme, *e.g.,* a current Acme processor, client, business partner or professional advisor, such as a law firm or auditor - Government Agency	Trustworthy Recipient - Third party with whom Acme does not have a contractual relationship, but who provides credible assurances that the data will not be misused (*e.g.*, a former vendor or client) - A regulated entity, such as a financial institution, insurance company or healthcare provider	Untrusted Recipient - Unknown recipient (*e.g.,* public disclosure or loss of data) - Recipients with known or suspected malicious intent (*e.g.,* theft of data)

THIS EVENT: Circle Rating Points: 0 1 2

EXPLAIN:_____

_____

3. Whether the personal data was actually viewed or acquired:

0 Points	1 Point	2 Points
Not viewed or acquired - Acme determines that file has been sent to the wrong recipient and retrieves the data prior to it being accessed. - Recipient reports receiving an incorrect file without viewing contents and deletes, returns or destroys the file without reading/copying/printing.	Viewed (or partially viewed) but not acquired - Recipient opens package or file but realizes that it has been incorrectly directed and deletes (returns or destroys) the file without using or further disclosing the information.	Acquired - Acme cannot recover the data from the recipient.

- Lost device/media is recovered, and forensic analysis confirms it was not accessed.		

THIS EVENT: Circle Rating Points: 0 1 2

EXPLAIN:_____

_____

4. The extent to which any risk to the personal data has been mitigated:

0 Points	1 Point	2 Points
Acme has a good faith reason to believe that personal data have not and will not be used, disclosed or retained. - Personal data have been fully recovered. Trusted or trust-worthy recipient has provided credible written assurances that the data has not been used or disclosed and that no instance of the data has been retained. - Personal data were encrypted and the encryption keys were not compromised.	Acme has a good faith reason to believe that personal data have not and will not be used or disclosed. - Personal data have been recovered from active recipient systems. Trusted or trust-worthy recipient has provided credible written assurances that the data has not been used or disclosed (but retention in back-ups may occur). - The trusted or trustworthy recipient has an established program to protect similar information internally.	No mitigation - Acme does not have any assurances regarding use, disclosure or retention of the personal data.

THIS EVENT: Circle Rating Points: 0 1 2

EXPLAIN: _____.

_____

Are there any other factors or information which can assist in determining if the personal data were compromised?

EXPLAIN:_____

_____

C. Calculate Score

Add the rating points from factors 1-4 above. **Total Score: ____**

Total score 7 or 8: The personal data have been compromised. *Comply with DPDPA Rule 7.*

Total score 5 or 6: The personal data may have been compromised. Acme's privacy office or legal counsel should review the facts and determine if breach notification is required.

Total score 4 or less: The personal data have not been compromised. Although there may be some risk factors (such as sensitive personal data on a stolen device), the probability of compromise must be low (such as if the data is encrypted). The likelihood that personal data have been compromised may also be low if the data were viewed by a trusted third party with appropriate mitigation of the event.