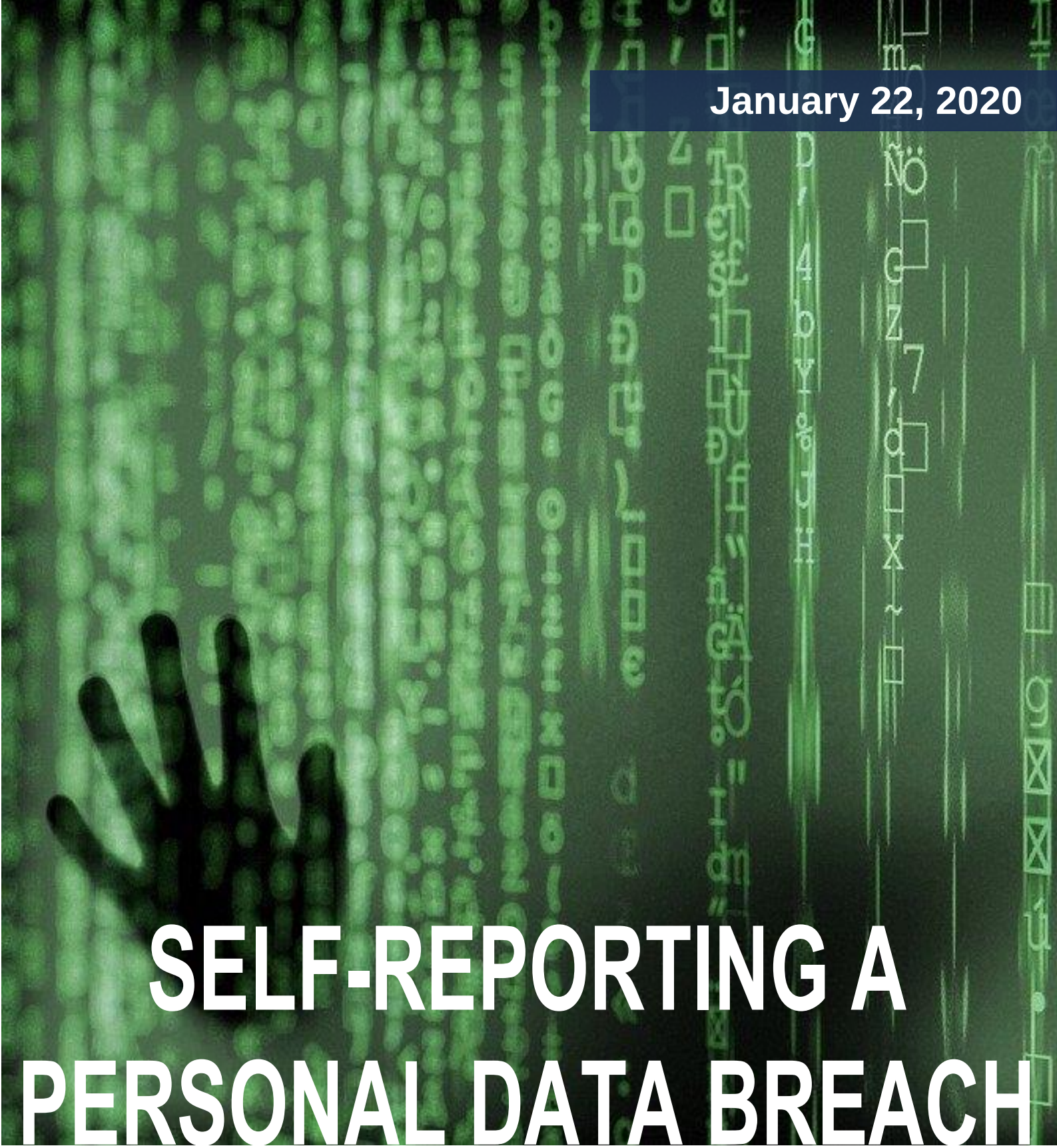

January 22, 2020

SELF-REPORTING A PERSONAL DATA BREACH

- AN OBLIGATION UNDER THE PERSONAL DATA PROTECTION BILL 2019

argus partners
SOLICITORS AND ADVOCATES

TECHNOLOGY & DATA PRIVACY

MUMBAI I DELHI I BENGALURU I KOLKATA I AHMEDABAD

Introduction

Imagine for a moment that traffic rules required every motorist and pedestrian to self-report any violation of traffic rules. If you violate any traffic rule, you have to inform the traffic police by filing an online report within 12 (twelve) hours of the violation. After you report, you will receive a suitable punishment, which could be a fine or imprisonment or both. The traffic police department may also publicise your violation, at its discretion, either by posting details of your violation on the traffic police department's website or by ordering you to stick a notice containing details of your violation on an outer wall of your dwelling or both. In case you fail to report and your violation is detected through any other means, be it a security camera or on account of any other motorist or pedestrian reporting an incident, you shall also, in addition to the penalty for your violation, be penalised for the failure to report.

Duty to Report

Section 25 of the Personal Data Protection Bill, 2019 ("**PDP Bill**") requires every data fiduciary to inform the Data Protection Authority of India ("**Authority**") by notice about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal. It is irrelevant whether the breach took place due to a fault on the part of the data fiduciary or not.

Definition of Personal Data Breach

A "personal data breach" has been defined by the PDP Bill to mean any unauthorised or accidental disclosure of, acquisition of, sharing of, use of, alteration of, destruction of, loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal. Though the PDP Bill does not expressly say so, it is likely to be presumed that the breach took place due to the failure of the data fiduciary to comply with the law and safeguard the personal data that was held by the data fiduciary or by a data processor reporting to the data fiduciary.

Time Limit

Sub-clause (3) of section 25 of the PDP Bill provides that the notice referred to in sub-section (1) shall be made by the data fiduciary to the Authority as soon as possible and within such period, as may be specified by the regulations made by the Authority under the PDP Bill, following the breach after accounting for any period that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm. After the PDP Bill comes into effect, we expect the government to frame regulations under this section to specify the time period within which the Authority has to be notified by the data fiduciary after a personal data breach takes place. Irrespective of such a time limit, the data fiduciary is obliged to notify the Authority as soon as possible after a breach has occurred.

Details to be reported

The notice sent by the data fiduciary is required to include particulars such as (a) the nature of personal data which is the subject matter of the breach, (b) the number of data principals affected by the breach, (c) the possible consequences of the breach and (d) the action being taken by the data fiduciary to remedy the breach. Sub-clause (6) of section 25 of the PDP Bill states that the Authority may also direct the data fiduciary to take appropriate remedial action as soon as possible and to conspicuously post the details of the personal data breach on its website. In any event,

each data fiduciary is under a duty to take all possible mitigatory steps after any personal data breach occurs.

It is possible that a data fiduciary may not have full details of the nature of personal data which is the subject matter of the breach or of the number of data principals affected by the breach or of the possible consequences of the breach. This would be the case, for example, when a burglary at a financial institution's data processing centre results in the theft of a number of laptops containing personal data relating to the financial institution's customers. The laptops might have been secured with passwords which make it impossible to access the personal data. If the financial institution is confident that the passwords cannot be breached, it may not report the incident since there would be no breach of personal data. However, if some of the laptops did not have adequate security, the theft of such laptops would have to be reported. It might take the financial institution many hours to figure out which of the stolen laptops were properly secured, which ones were not and what personal data was contained in the unsecured laptops. It is for this reason that sub-clause (4) of section 25 of the PDP Bill provides that where it is not possible to provide all the required information, at the same time, the data fiduciary shall provide such information to the Authority in phases without undue delay. Thus, details of the breach have to be reported to the Authority, as soon as possible, giving whatever details are available with the data fiduciary. As more information becomes available, further reports have to be filed. In any event, a report has to be filed within the prescribed time, with whatever information is available to the data fiduciary.

Action by the Authority

Upon receipt of a notice, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm.

The Authority may require the data fiduciary to post details of the personal data breach on the data fiduciary's website. The Authority may also post details of the data fiduciary's personal data breach on its own website.

Further, once a breach of personal data is brought to the Authority's notice, the reasons for the breach will presumably be analysed and action will be initiated against the data fiduciary under applicable laws for any violation of such laws. As mentioned above, it is likely that any breach of personal data will create a presumption that the data fiduciary, or any data processor reporting to the data fiduciary, failed to comply with the law and safeguard the personal data that was held by the data fiduciary or the data processor, as the case may be. The data fiduciary would have to overcome such presumption by providing sufficient information to the Authority to convince the Authority that the breach of personal data took place without the data fiduciary, or any data processor reporting to the data fiduciary, having been in breach of any applicable law or regulation.

Consequences of Failure to Report a Breach of Personal Data

As per section 57(1)(a) of PDP Bill, in the event the data fiduciary contravenes its obligation to take prompt and appropriate action in response to a data security breach under section 25 of the PDP Bill, such data fiduciary shall be liable to a penalty which may extend to Rs. 50,000,000 (Rupees fifty million) or 2% (two percent) of its total worldwide turnover of the preceding financial year, whichever is higher.

Section 57 of the PDP Bill clarifies that that the expression "*total worldwide turnover*" means the gross amount of revenue recognised in the profit and loss account or any other equivalent statement, as applicable, from the sale, supply or distribution of goods or services or on account

of services rendered, or both, and where such revenue is generated within India and outside India. It further clarifies that the total worldwide turnover in relation to a data fiduciary is the total worldwide turnover of the data fiduciary and the total worldwide turnover of any group entity of the data fiduciary where such turnover of a group entity arises as a result of the processing activities of the data fiduciary, having regard to factors, including:

(a) the alignment of the overall economic interests of the data fiduciary and the group entity;
(b) the relationship between the data fiduciary and the group entity specifically in relation to the processing activity undertaken by the data fiduciary; or
(c) the degree of control exercised by the group entity over the data fiduciary or vice versa, as the case may be.

Comparison with GDPR

Article 33 of the General Data Protection Regulation ("**GDPR**") deals with notification of data breach and is very similar to section 25 of the PDP Bill. Article 33 of GDPR requires any breach to be reported without undue delay and where feasible, within 72 (seventy two) hours after having become aware of it. Unlike Article 33 of GDPR, section 25 of the PDP Bill does not state that the clock will start ticking once the data fiduciary become aware of the breach. Section 25 of the PDP Bill requires the data fiduciary to notify the Authority as soon as possible after a breach has occurred. The words "as soon as possible" would imply that the data fiduciary should have become aware of the breach. However, the final deadline (which will possibly be specified in the rules to be framed) is not subject to the data fiduciary's knowledge. It is possible that the rules to be framed will press the stopwatch for the deadline from the time the data fiduciary becomes aware of the breach.

Interestingly, Article 34 of the GDPR deals with communication of personal data breach to the data subject and provides that when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is required to communicate the personal data breach to the data subject without undue delay. There is no similar provision in the PDP Bill that requires the data fiduciary to directly communicate a personal data breach to the data principal. The communication that is required to be made directly to the data subject under Article 34 of the GDPR shall contain the same type of information as is required to be reported to the supervisory authority under Article 33 of the GDPR. However, Article 34 of the GDPR also provides that the communication to the data subject under Article 34 shall not be required if: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects are no longer likely to materialise; or (c) it would involve disproportionate effort. In the event the communication involves disproportionate effort, Article 34 of the GDPR provides that there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Further, like the PDP Bill, Article 34(4) of the GDPR provides that in the event the controller has not already communicated the personal data breach to the data subject in accordance with Article 34 of the GDPR, the supervisory authority may require the controller to do so. Under Article 58(2) of the GDPR, the supervisory authority, *inter alia*, has the power to issue reprimands to a controller or a processor where processing operations have infringed the provisions of the GDPR and to order the controller or processor to bring processing operations into compliance with the provisions of the GDPR where appropriate, in a specified manner and within a specified period. However, under the GDPR the supervisory authority does not have the power to either order the controller to post details of the personal data breach on the controller's website or to post details of the breach on its own website.

When does the Duty to Report a Personal Data Breach arise under the PDP Bill?

As mentioned above, not all breaches of personal data have to be reported to the Authority. Under section 25 of the PDP Bill, a data fiduciary is required to notify the Authority of any personal data breach where such breach is likely to cause harm to any data principal. The use of the word 'likely' makes it clear that the data fiduciary does not have to be absolutely sure that the breach will cause harm to one or more data principals. The likelihood of harm is sufficient. However, even "likelihood" is a subjective concept and can lead to confusion and possible disputes with the Authority.

When does the Duty to Report a Personal Data Breach arise under GDPR? - Regulatory Advice from the UK

The Information Commissioners Office ("**ICO**"), the independent authority set up in the United Kingdom to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals, on its website provides clarity on what data breaches are required to be disclosed. The ICO website, *inter alia*, provides as follows:

"*What breaches do we need to notify the ICO about?*

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Example

The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.

So, on becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen."[1] (emphasis supplied)

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

The ICO website also provides certain examples of a personal data breach, which include the following:

(a) access by an unauthorised third party;
(b) deliberate or accidental action (or inaction) by a controller or processor;
(c) sending personal data to an incorrect recipient;
(d) computing devices containing personal data being lost or stolen;
(e) alteration of personal data without permission; and
(f) loss of availability of personal data.

The ICO website also provides a self-assessment test to help determine whether an organisation needs to report a data breach to the ICO.[2]

Examples from the European Union

1. British Airways

Users of the British Airways ("**BA**") website were diverted to a fraudulent website where details of 500,000 (five hundred thousand) customers were acquired by the hackers. The incident was first reported on September 6, 2018, and initially, BA had reported that 380,000 (three hundred eighty thousand) transactions were affected but that the data that was breached did not include passport or travel details. The ICO found that a variety of information was "compromised" by poor security arrangements at BA, including log in, payment card, and travel booking details as well name and address information. The ICO had also stated that BA had co-operated with its investigation and made improvements to its security arrangements. BA was charged a penalty of 1.5% (one point five percent) of its worldwide turnover in 2017 amounting to approximately GBP 183,390,000 (British Pound Sterling one hundred eighty three million three hundred ninety thousand).

2. Google

After it emerged that Google Inc.'s smart speaker was unintentionally recording users' conversations, the data protection commission investigated reports of a potential data breach at Google Inc. ("**Google**"). Google made the breach notification in accordance with the GDPR.

Separately, a fine of € 50,000,000 (Euros fifty million) was imposed by the French data protection authority (Commission nationale de l'informatique et des libertés) on Google on the basis of complaints from an Austrian organisation and a French non-governmental organisation on May 25, 2018, and May 28, 2018, regarding the creation of a Google account during the configuration of a mobile phone using the Android operating system. Lack of transparency, insufficient information and lack of legal basis were cited when the aforesaid penalty was imposed. The aforementioned fine of € 50,000,000 (Euros fifty million) is the highest fine ever imposed any data protection authority under GDPR till date.

3. Hungarian Political Party

The Hungarian National Authority for Data Protection and the Freedom of Information ("**NAIH**"), the supervisory authority in Hungary, imposed a fine of € 34,375 (Euros thirty four thousand three hundred seventy five) on an undisclosed Hungarian political party for failing to notify the NAIH about a data breach and for failing to document the data breach in accordance with Article 33 of the GDPR. The fine was based on 4% (four percent) of the party's annual turnover and 2.65 % (two point six five percent) of its anticipated turnover for

[2] https://ico.org.uk/for-organisations/report-a-breach/pdb-assessment/

the coming year. The breach, in this case, was as a result of a cyber attack by a hacker who accessed and disclosed information on the vulnerability of the party's system which was a database that contained the information of more than 6,000 (six thousand) individuals. It was disclosed that the system was vulnerable to attack due to a redirection problem with the webpage. After the command was shared, people with very little technological knowledge were also able to retrieve information from the database.

4. Payment Service Provider UAB MisterTango

During an inspection, the Lithuanian Data Protection Supervisory Authority found that UAB MisterTango, a data controller, processed more data than was necessary to achieve the purposes for which such data had been collected. It was also found that from July 2018, payment data was publicly available on the internet due to inadequate technical and organisational measures. 9,000 (nine thousand) payments with 12 (twelve) banks from different countries were affected. The supervisory authority stated that a data breach notification pursuant to Article 33 of the GDPR would have been necessary for such inadequate technical and organisational measures. UAB MisterTango had not reported the data breach and therefore a penalty of € 61,500 (Euros sixty one thousand five hundred) was imposed on UAB MisterTango.

5. Facebook

Hackers were able to take advantage of a vulnerability in Facebook Inc.'s "View As" feature and steal the access tokens for approximately 50,000,0000 (fifty million) users which allowed the hackers to take over users' accounts. Facebook Inc. ("**Facebook**") discovered the vulnerability on September 26, 2018, and reported the same within the 3 (three) day limit. However, Facebook did not share all the pertinent details with the relevant data protection authority, in this case, the Irish Data Protection Commission ("**IDPC**"). In December 2018, Facebook was forced to issue a notification that another bug had exposed 6,800,000 (six million eight hundred thousand) users' private photos to up to 1,500 (one thousand five hundred) different applications for nearly 2 (two) weeks. This bug had been discovered and fixed on September 25, 2018, but, Facebook had not alerted affected users, the public, or authorities for almost 3 (three) months. Facebook stated that they were carrying out their own investigation in order to conclude whether the same was a reportable breach under the GDPR and reported the same within 72 (seventy two) hours of concluding the same. The investigation into this breach is still ongoing.

Parallels in Other Indian Laws

The duty to self-report a breach can be found in various regulations framed by the Securities and Exchange Board of India ("**SEBI**") and the Reserve Bank of India ("**RBI**"). For example:

1. The RBI has, vide a notification dated June 2, 2016 made it mandatory for banks to report all unusual cybersecurity incidents within 2 (two) to 6 (six) hours of discovery (whether they were successful or were attempts which did not fructify) to the RBI and to the Indian Banks – Center for Analysis of Risks and Threats (IB-CART). As per the notification, the RBI believes that such reporting shall help the banks in obtaining collective threat intelligence, timely alerts and adopting proactive cyber security measures.

2. As per SEBI's regulations for alternative investment funds ("**Funds**"), the manager of each Fund is required to prepare a compliance test report on compliance with SEBI's regulations for Funds. The compliance test report is required to be shared with the Fund's trustee and/or sponsor. In case any violation of the regulations or circulars issued in relation to

Funds is observed by the trustee/sponsor, SEBI is required to be intimated as soon as possible[3].

However, mandating that regulated financial institutions report any breach to their regulator is very different from calling on data fiduciaries of all hues to self-report any breach. As mentioned above, the PDP Bill has taken a leaf from the GDPR booklet in this regard. However, once the PDP Bill comes into effect, many individuals and organisations, will be bound to comply with a complicated set of rules regarding the processing of personal data and the duty to self-report any breach (which may or many not have taken place due to a fault on the part of the data fiduciary) will be one of the various onerous duties being thrust on to them under this new legislation.

This paper has been written by Vinod Joseph (Partner) and Deeya Ray (Associate).

[3] SEBI circular dated June 19, 2014 bearing number CIR/IMD/DF/14/2014

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
argusknowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata

www.argus-p.com