Comments on the draft rules made by the Central Government of India under sub-sections (1) and (2) of section 40 of the Indian Digital Personal Data Protection Act, 2023 submitted by the City of London Law Society Data Law Committee.

Version date: 9 February 2025

About the City of London Law Society and the Data Law Committee

The City of London Law Society ("CLLS") represents approximately 21,000 City of London lawyers through individual and corporate membership including some of the largest international law firms in the world. These law firms advise a variety of clients from multinational companies and financial institutions to government departments (UK and otherwise), often in relation to complex, multijurisdictional legal issues. The CLLS responds to a variety of consultations on issues of importance to its members through its' 22 specialist committees.

This response has been prepared by the CLLS Data Law Committee (the "Committee") whose members comprise London City lawyers specialising in data protection law. Many of the members advise multinational clients who count Indian ITO and BPO companies among their valued suppliers and in some cases who have established shared services centres or other operations in India. The Data Law Committee therefore has a keen interest in the development of Indian data protection laws and their interplay with data protection laws in other jurisdictions, notably those in the UK and Europe.

We welcome the opportunity to respond to the draft rules made by the Central Government of India under sub-sections (1) and (2) of section 40 of the Indian Digital Personal Data Protection Act, 2023. This submission is not confidential and we have no objection to it being published. Opinions in this response are those of the members of the CLLS Data Law Committee and do not necessarily represent the opinions or views of the CLLS.

If you have any questions, please contact:

Jonathan Bartley, Chair, CLLS Data Law Committee, jon.bartley@rpclegal.com;

Ross McKean, Member, CLLS Data Law Committee, ross.mckean@dlapiper.com, and

Kevin Hart, legal policy analyst, CLLS, kevin.hart@clls.org.

***

Rule 1 (2) and (3): Commencement of the rules

Rule 1 currently states that the rules will come into effect from the date of publication of the final rules in the Official Gazette but that rules 3-15, 21 and 22 will come into effect at a later, unknown date.

We recommend that a transition period of at least two years is factored into Rule 1 to enable stakeholders (particularly small and medium sized enterprises) to adapt and comply with the Rules.

Rule 3. Notice given by Data Fiduciary to Data Principal

The draft rule only seems to contemplate the scenario where personal data are collected directly by the Data Fiduciary from the Data Principal which in the hyperconnected digital world is not always the case. **We recommend** addressing fair processing notice requirements discretely for both (i) scenarios where personal data are collected directly from the Data Principal; and (ii) scenarios where personal data are collected indirectly from the Data Principal. Similar to the approach taken in Articles 13 (direct) and 14 (indirect) of the EU General Data Protection Regulation (GDPR).

There are certain data flows which support progressive services which are clearly in the public interest such as credit reference, authentication and fraud prevention checks where personal data are frequently obtained from third party sources rather than direct from the individual and provision of transparency information to the individual is therefore more challenging. To ensure that these services and the data flows that support them can continue to thrive **we recommend** including a similar discrete set of transparency requirements as those set out in Article 14 GDPR.

Further **we recommend** that consideration is given to the means in which the notice must be provided by the Data Fiduciary to the Data Principal in circumstances where the Data Fiduciary obtained the personal data indirectly and does not have contact details of the individual. In this scenario, **we recommend** a similar approach to that set out in Article 14(5)(b) of the GDPR, i.e. where the provision of the notice proves impossible or would involve a disproportionate effort, then the Data Fiduciary may instead publish the information required in draft Rule 3 on its own or a third party's website (or by other public means).

There is a linked point here which is the wider question of alternative lawful bases to legitimise processing of personal data, i.e. other than consent. For some data flows and use cases, particularly those involving the collection of personal data from third parties rather than from the Data Principal themselves, it is likely to be challenging to obtain valid consent and for that reason privacy laws in other jurisdictions have developed other lawful bases including, for example, the legitimate interests of the Data Fiduciary where those interests are not outweighed by the rights and interests of the Data Principal. There is a risk that limiting the lawful basis to consent in most cases will hamper innovation and the development of progressive services many of which could help to protect Indian citizens from harm, such as authentication services used for fraud detection and prevention.

Where consent is used as the lawful basis for processing, Section 5(2) of the DPDP Act indicates that if a Data Fiduciary has already obtained consent from a Data Principal to process their personal data before the commencement of the DPDP Act, the Data Fiduciary will be able to continue such processing until the Data Principal withdraws their consent so long as that the Data Fiduciary provides the Data Principal with a notice that meets the requirements of the DPDP Act and the Rules (i.e. a notice provided in accordance with Rule 3).

While Rule 3 sets out the details that the Data Fiduciary needs to include in the notice, **we recommend** that Rule 3 clarifies whether all forms of consent obtained prior to the commencement of the DPDP Act constitute valid consent for the purposes of Section 5(2) or whether the consent needs to meet the consent standards specified in Section 6 in order to be deemed valid.

If it is the latter, **we recommend** that Rule 3 confirms that a Data Fiduciary needs to obtain fresh consent from the Data Principal where an existing consent it has obtained does not meet the consent standards of Section 6 (rather than just providing them with the notice under Rule 3).

Rule 6: Reasonable security safeguards

We agree with the technology neutral approach taken in the draft Rule 6. Further guidance would be welcome as to what specific security is required in practice and **we recommend** that such guidance specifically refers out to recognised and widely adopted international information security standards such as ISO 27001 and the US NIST Cyber Security Framework.

In relation to Rule 6(1) and Rule 6(1)(a) to (g), the drafting could be interpreted as stating that, in *all* cases, all of the specific measures set out in 6(1)(a) to (g) must be implemented, irrespective of the volume or sensitivity of the data, or the risk of harm to Data Principals. This could impose a disproportionate burden on Data Fiduciaries with limited practical benefit for Data Principals. We would propose that the drafting is clarified so that the reference to the specific measures in Rule 6(1)(a) to (g) are illustrative examples to be implemented "where appropriate" but not mandatory in all cases. This could be resolved by replacing "at the minimum" with "where appropriate" at the end of the run-in language in Rule 6(1) and updating Rules 6(1)(a) to (g) by removing the redundant references to "appropriate". Or alternatively "where appropriate, having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the likelihood and severity of risk of harm to Data Principals…" similar to the language used in Article 32 GDPR which has been followed in various derivative laws in other jurisdictions and is a familiar concept to multinational organisations.

Rule 7: Intimation of personal data breach

7(1). There is no harm threshold. As currently drafted rule 7(1) would require *any* personal data breach, irrespective of its seriousness, to be notified to each affected Data Principal.

This will likely lead to multiple notifications of trivial breaches in turn leading to "notification fatigue" and risks Data Principals ignoring notices they receive for genuinely serious and harmful breaches. It also risks distracting Data Fiduciaries and wasting finite time and resources which could be better spent on addressing other – more material - compliance requirements.

By comparison, the EU GDPR only requires notification to data subjects (the equivalent of Data Principals) where the breach is likely to result in a "high risk to the rights and freedoms" of natural persons (Article 34(1) GDPR). The Swiss federal data protection law limits the obligation to notify impacted individuals even further, only requiring notification if this is required for their protection or if the Swiss data protection authority so requests (Article 24(4) Swiss Federal Act on Data Protection of 25 September 2020). The Swiss legislature had the benefit of seeing how the EU GDPR notification obligations played out in practice (as the Swiss law came into force several years after the EU GDPR applied) which no doubt influenced their decision to raise the bar for notification to individuals. In addition to the risk of over-notification fatigue, there is also the risk of causing unnecessary alarm to impacted Data Principals where there is nothing that they can do about the risks presented by the breach. Receiving a notification can cause mental distress so notifications should be limited to where the harm of not notifying outweighs the mental anguish caused by notifying.

Taking the above considerations into account **we recommend** limiting the obligation to notify Data Principals in rule 7(1) where the following two conditions are met: (i) the personal data breach is likely to result in a high risk of harm to the Data Principal; and (ii) notification will allow the Data Principal to take protective steps.

Rule 7(1). There is a lack of appropriate exemptions to the notification obligation. As currently drafted, Rule 7 is a blanket requirement to notify even in circumstances where there cannot be any harm to the impacted Data Principals and even where it is technically impossible or disproportionately burdensome to make the notification, for example where contact details are either missing, incorrect or out of date.

To address these issues **we recommend** adding the following exemptions to the requirement to notify under Rule 7(1) with a view to reducing the risk of notification fatigue, disproportionate burden on Data Fiduciaries and causing unnecessary alarm to Data Principals. These exemptions mirror similar exemptions in Article 34(3) GDPR:

- No notification should be required where the Data Fiduciary 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;

- No notification should be required where the Data Fiduciary has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Principals is no longer likely to materialise;

- No notification should be required to individuals (e.g. by post / email / phone / in person) where this would involve disproportionate effort. In such cases the Data Fiduciary should instead make a public communication or similar measure whereby the Data Principals are informed in an equally effective manner[1].

Rule 7(1). Additional proposals

If the recommendations above are implemented in the final Rules, then **we recommend** that the Board retains the power to demand that a Data Fiduciary notify Data Principals of a personal data breach if the Data Fiduciary has not yet notified where the Board determines, having regard to all the circumstances of the personal data

[1] This is sometimes referred to as "substitute notice" in the USA and is common practice where either there are no contact details held on file for a Data Principal or the contact details are wrong / out of date. Examples of public communications may include website notices and/or adverts in national or media newspapers (digital and/or hard copy).

breach, that it is likely to result in a high risk of harm to Data Principals. Similar powers are included in both the GDPR (Article 34(4)) and in the Swiss Federal Act on Data Protection (Article 24(4)).

Rule 7(2). Intimation of personal data breach to the Board. This requirement should take primacy over the obligation to notify impacted Data Principals.

The approach taken in GDPR, the Swiss Federal Act on Data Protection and many similar laws in other jurisdictions is to set a lower bar for notification to the data protection regulator than the bar set for notification to impacted individuals. The logic being that there are public policy reasons for regulators to have wider visibility of personal data breaches whereas not all personal data breaches cause harm so not all should be notified to impacted individuals. Giving primacy to the obligation to intimate personal data breaches to the Board rather than first notifying impacted Data Principals (irrespective of actual harm) would also help to avoid the situation of reputational harm to the Data Fiduciary from social media or mainstream media coverage which is more likely where Data Principals are notified of personal data breaches. For more serious breaches, media coverage is to be anticipated and is appropriate but as currently drafted there is a risk of media coverage (and reputational harm) arising from trivial personal data breaches where there is no risk of harm to impacted Data Principals.

We recommend reversing rule 7(1) and 7(2) so that the obligation to notify personal data breaches to the Board is the primary obligation.

Similar to Rule 7(1), there is no harm threshold for the requirement to notify personal data breaches to the Board.

We recommend that the requirement to notify personal data breaches to the Board is qualified so that notification is not required where the Data Fiduciary has assessed that the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals (similar to Article 33(1) GDPR). This should help to reduce the number of personal data breaches notified to the Board and exclude the genuinely trivial.

You might also consider taking this reasoning a step further and limiting the requirement to notify personal data breaches to the Board only to those breaches where there is likely to be a high risk of harm to impacted individuals. This is the approach taken by the Swiss Federal Act on Data Protection (Article 24(1)). The alternative is for the Board to have to deal with triaging likely thousands of personal data breach notifications every year which risks becoming a distraction to dealing with serious breaches. There is also the risk that more serious breaches will be lost in the "noise" of thousands of personal data breach notifications.

Rule 7(2). 72 hour timeline for provision of detailed information is unrealistic. The detailed information which the Data Fiduciary is required to intimate to the Board will inevitably take a lot longer than 72 hours to compile leading to requests for extension becoming the norm and becoming an unwelcome distraction when a victim Data Fiduciary is dealing with a serious personal data breach. Multiple requests for extension risk overwhelming the Board. As just one example, forensic investigations into the root causes of breaches often take weeks and sometimes months. Similarly, eDiscovery exercises reviewing exfiltrated personal data to determine which Data Principals it relates to and what specific personal data attributes have been exfiltrated for each individual can take several months to complete, particularly with unstructured data sets and even with the help of AI.

We recommend adding a qualification to the 72 hour timeline to the effect that where it is not possible to provide the information within the 72 hour period then the information may be provided in phases, without undue further delay. This is similar to the approach taken in Article 33(4) GDPR.

Rule 7(2). Additional proposals. The draft rules are silent regarding the role of a Data Processor in the event that they discover a personal data breach impacting personal data controlled by one or more Data Fiduciaries. This could lead to confusion. Once the Data Fiduciary is notified by the Data Processor of a personal data breach it would then need to assess whether notification is required to the Board and/or impacted Data Principals. But this should remain the responsibility of the Data Fiduciary, not the Data Processor.

We recommend that an obligation is added to Rule 7 that a Data Processor shall notify the Data Fiduciary without undue delay after becoming aware of a personal data breach. This is similar to the approach taken in Article 33(2) GDPR.

Rule 12. Additional Obligations of Significant Data Fiduciary

The definition of "Significant Data Fiduciary" as set out in the Digital Personal Data Act, 2023 (Chapter I, Section 2(z) and Section 10) do not appear to be intended to cover either Indian information technology vendors or business process vendors offering services to customers outside of India, nor to captive shared service centres owned by overseas companies which provide services to those companies from India. However, it would be helpful if further guidance could be provided to confirm that these entities are not Significant Data Fiduciaries. Particularly given the proposed data localisation requirements in draft rule 12(4).

Rule 13(3). Rights of Data Principals

As currently drafted this reads as allowing Data Fiduciaries quite a wide discretion to determine the period under their grievance redressal system for responding to the grievances of Data Principals which could lead to a wide variety of different approaches and confusion both for Data Principals and for Data Fiduciaries trying to determine what the legal standard of care is. It would be helpful if more clarity was provided here regarding the time permitted for substantive response to Data Principals seeking to exercise their rights. As a benchmark, GDPR allows up to 3 months.

Rule 22. Calling for information from Data Fiduciary or intermediary

Laws and regulations which restrict of prohibit the transfer of personal data from organisations outside India which use or wish to use Indian based vendors or shared service centres for IT, business process outsourcing and other services present a significant headwind to the continued success of this important and economically significant sector in India. Organisations within the EU and UK have a particularly high bar to meet under GDPR for risk assessments when transferring personal data from within the EU or UK to "third countries" such as India. While we appreciate that it is the sovereign right and a necessity for India to have the power to access information for legitimate purposes such as law enforcement, Indian laws permitting access by public authorities are currently extremely widely drawn with limited oversight which makes it harder for organisations wishing to engage Indian suppliers or to invest in Indian service centres, to justify exports of personal data to India. It is notable that the concept of "transfer" as it is interpreted by UK and EU regulators is extremely broad and includes mere remote access from India. Storage of personal data in India is not a pre-requisite to a data flow falling within the broad concept of "transfer" under GDPR.

Given the call for comments on the Rules and the current focus on data and interception laws by the Central Government it may therefore be timely to consider a wider review of these powers with a view to, on the one hand, ensuring that Indian government and law enforcement authorities have the powers they need to access information for defined legitimate purposes and on, the other hand, to ensure that there are appropriate guardrails and oversight for the exercise of these powers which in turn should help UK and EU based organisations which wish to transfer personal data to India and who therefore typically need to complete transfer impact assessments.

Section 36 of the Digital Personal Data Protection Act, 2023 (**DPDP Act**) read with Rule 22 provides the Central Government the power to demand any "*information as may be called for*" from a Data Fiduciary or an intermediary (as defined in the Information Technology Act 2000 (**IT Act**)), for the purposes listed in the Seventh Schedule of the Rules. The IT Act adopts a very broad definition of “intermediary” – essentially including any provider of digital services entitled to process personal data. The purposes listed in the Rules are also very broad and include a number of vague concepts. In particular, the first purpose of the Seventh Schedule allows the State or any of its instrumentalities to call for the personal information of individuals in the interest of the "sovereignty and integrity" of India or the "security of the State". These broad concepts, which are not defined, leave a significant level of discretion to the Central Government.

In addition, the DPDP Act allows Central Government to exempt itself from the provisions and safeguards within the DPDP Act, with little oversight or requirement for proportionality.

As the information to which the Central Government may have access may include personal data of individuals in the UK and the EU, Rule 22 is likely to impact the ability of organisations in the UK and the EU to transfer personal data to businesses in India and, in particular, may impact the risk rating when carrying out transfer impact assessments (required to be carried out by European organisations when transferring personal data to

India). The European Data Protection Board has specifically raised concerns in this regard, finding, in its report[2] on government access to data in third countries, that "*[Indian] legislation provides for widespread exemptions for governmental access to personal data with little or no guarantees for the data subjects*".

Taking the above into account, in order to potentially lower the risk for UK and EU organisations transferring personal data to India and therefore mitigating a headwind to the use of Indian suppliers and Indian shared service centres, **we recommend** clarifying the meaning of "*information as may be called for",* in particular whether 'information' includes the personal data of individuals (including personal data of EU individuals). In addition, **we recommend** further clarifying the purposes listed in Seventh Schedule of the Rules to ensure that (i) any public authority access to personal data is carried out in pursuit of legitimate aims which are both necessary and proportionate in a democratic society; and (ii) that public authority access is subject to adequate and effective oversight from courts or other independent authorities. While beyond the scope of the current consultation **we recommend** a wider review of the powers allowing public authorities in India to access information, including personal data, to ensure that appropriate guardrails and oversight are in place in line with evolving best practice and informed by the now quite extensive jurisprudence considering the GDPR restrictions on international transfers of personal data.

***

[2] legalstudy_on_government_access_0.pdf