guarantees such as respect for individual privacy, protection of personal data and principles of privacy. The Joint Declaration proposes closer cooperation between the Countries on promoting high data protection and privacy standards based on core elements such as:

1. Comprehensive legal frameworks and policies applicable to public and private sectors;
2. Key data protection principles such as purpose limitation, data minimization, transparency, data security and accountability;
3. Individual rights such as access, rectification, deletion and safeguards in relation to automated decision making;
4. Safeguards for cross-border transfers; and
5. Independent oversight by supervisory authorities and effective redressal.

Proposed cross-border data transfer restrictions

Interestingly, the Joint Declaration comes months after the Joint Committee on Personal Data Protection Bill, 2019 ('**JPC**') recommended numerous changes to a 2019 draft (the Personal Data Protection Bill, 2019) ('**2019 Bill**') and proposed the Data Protection Bill, 2021 ('**Bill**'). The Bill proposes cross-border transfer of Sensitive Personal Data[2] ('**SPD**') subject to certain transfer grounds such as approved contracts or intra-group schemes, adequacy findings or permission for specific SPD or class of SPD for any purpose, in addition to explicit consent for transfer.[3] More limited grounds are proposed for transfers of critical personal data[4] (*which is not yet defined*).

The Joint Declaration provides that the Countries would foster cooperation on safeguards that enable cross-border data flows by ensuring that 'protection travels with the data'. While much clarity has not been provided on the nature of protection and safeguards, this may include protection achieved through standard pre-approved contracts or intra-group schemes or adequacy for a particular jurisdiction.

While the positions under the Bill appear to be broadly in line with the objectives outlined under the Joint Declaration, certain changes proposed by the JPC appear to be creating more uncertainties in light of the Joint Declaration:

---

a) Pre-approved Contracts: Cross-border transfers outside India on the basis of approved contracts (or intra-group schemes) contemplated under the 2019 Bill appeared to be similar to GDPR's standard contractual clauses[5]. However, pursuant to changes by the JPC, the Bill specified that approval of the contract (or intra-group scheme) be conditional on the object of transfer being compatible with public policy or State policy, thus implying that each contract (or scheme) may be subject to a case-by-case analysis, as opposed to relying on a legally prescribed approach, such as standard templates for data sharing/transfer agreements.

This may not be best suited for facilitating large flows of information across borders and may prove to be a hindrance to ease of business. Should standardized mechanisms be relied on, any obligations to 'public policy or state policy' may create subjectivity and pose compliance challenges.

---

b) Rights related to automated processing: A pertinent variance may also be observed in the case of personal data processed using automated means and individuals who have been subject to decisions as a result of such processing. The Bill provides for a right of data portability where data processing has been carried out through automated means, however, it does not expressly provide any right or safeguards against automated decisions.

On the other hand, the Joint Declaration provides for enforceable rights of individuals and safeguards with respect to automated decision-making and possibility to challenge the outcome. An earlier Report of the Committee of Experts[6] ('**Report**') discussed the merits of including a right to object to automated decision-making.[7] While the committee recognized it as a legitimate response to emerging challenges from big data and artificial intelligence, it argued that including a mere human review would not make a decision immune from prejudice and proposed inclusion of an *ex-ante* accountability framework requiring data fiduciaries making evaluative decisions to set up processes through privacy-by-design policies to weed out discriminative outcomes, observing that individual rights to approach courts exists in instances of discrimination. However, these rights may be better facilitated through regulatory frameworks, as opposed to courts, and the presence of a right to object may weed out obvious automated processing failures.

---

c) Sharing with foreign governments or agencies: The Bill also requires adequacy decisions to be issued on the basis of data protection laws, enforcement of laws by authorities and on the condition that such SPD may not be accessed by or shared with foreign governments or agencies unless approved by the Central Government.[8] While the specifics around enforcement of the provision remains unclear, this is similar to the requirement under the Personal Information Protection Law[9] ('PIPL') and the Data Security Law[10] ('DSL') in China which restrict transfer of personal data to foreign law enforcement or judicial authorities without prior approval of Chinese authorities.

Such obligations are not only onerous but also unreasonable to facilitate free flow of cross-border data and may also be challenging to enforce. This is particularly so, in the context of the Bill, as the Government issues adequacy decisions on the basis of similar data protection laws, safeguards, enforcement and agreements with different countries and may contemplate such situations when issuing such decisions.

Incoming Data and Data Transfer Impact Assessments

The Joint Declaration may also be relevant to take into consideration when assessing data transfers to India in the context of the new Standard Contractual Clauses[11] ('**SCC**') under the GDPR. The SCCs require parties to ensure that laws and practices of third countries respect fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society[12]. This is also reflected in the criteria for adequacy decisions[13] under the GDPR. The criteria for issuing adequacy decisions under the GDPR require assessment of the level of protection and to take into account the international commitments of the country or organization, obligations arising from conventions, instruments or participation in multilateral, bilateral or regional systems in relation to protection of personal data.[14]

The Joint Declaration may be relevant in data protection impact assessments as a positive step towards commitment to personal data protection and secure data subject rights, apart from international cooperation and convergence in privacy regimes. While it may not be a binding international instrument or agreement at this stage, it may go along a long way in establishing a multilateral system of reciprocal treatment and safeguards for protection of personal data and facilitate smooth cross-border data flows between the Countries.

[The authors are Senior Associate and Partner, respectively, in Data Protection practice team in Lakshmikumaran & Sridharan Attorneys, New Delhi]

[1] Joint Declaration on Privacy and Protection of Personal Data, available at https://mea.gov.in/bilateral-documents.htm?dtl/35001/Joint+Declaration+on+privacy+and+the+protection+of+personal+data+Strengthening+trust+in+the+digital+e

[2] Section 3(41) provides that sensitive personal data includes financial data, health data, official identifiers, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste, tribe, religious or political belief or affiliation or any other data categorized as sensitive personal data.

[3] Section 34, Data Protection Bill, 2021.

[4] Section 33, Data Protection Bill, 2021

[5] Article 46, General Data Protection Regulation, 2016.

[6] Report of the Committee of Experts, available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

[7] Article 22, General Data Protection Regulation, 2016.

[8] Section 34, Data Protection Bill, 2021.

[9] Article 41, Personal Information Protection Law, 2021

[10] Article 36, Data Security Law, 2021

[11] Standard Contractual Clauses for International Transfers dated June 4, 2021, available at https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf

[12] Clause 14(a), Standard Contractual Clauses.

[13] Article 45, General Data Protection Regulation, 2016.

[14] Recital 105, General Data Protection Regulation.

BROWSE ARTICLES

PRACTICE AREAS

MONTH

YEAR

Show

L&S NEWSLETTERS

your work email here

SUBSCRIBE