Published on *The National Law Review* https://www.natlawreview.com

Data Localization and Data Transfer Restrictions

Article By:

Elizabeth (Liz) Harding

Lisa J. Acevedo

Lindsay R. Dailey

In the modern global economy, data is the most valuable resource. Businesses use data to create value for customers and increase profit for its stakeholders. Although these businesses can only maximize their use of the data when it can flow freely across borders, many countries have been enacting measures that would make transferring data more complicated, expensive, time consuming, and at times, illegal.

Data Localization vs. Data Transfer

Data localization laws govern the location where personal data is stored, whereas data transfer laws govern the ability to disclose copies of personal data outside the borders of a country or region, but do not require local storage. Often, data localization laws incorporate aspects of data transfer laws. Globally, these rules are not uniform and many countries have adopted their own requirements which can vary based on the types of personal data covered and the scope of their respective requirements. The following are the most commonly seen categories of data localization and data transfer laws:

1. **Broad Localization Laws:** Cover all categories of personal data and a copy of the data must be stored in country. Cross border transfers are permitted under certain exceptions.

2. **Specific Localization Laws:** Cover specific categories of personal data and/or certain types of organizations which must comply, and a copy of the data must be stored locally. Cross border transfers are permitted under certain exceptions.

3. **Combined Localization/Transfer Laws:** Cover specific categories of personal data, and the data must be stored locally unless an exception applies. These types of laws typically do not require storing a copy of the data locally, and cross border transfers are permitted under certain exceptions.

4. **Pure Data Transfer Laws:** Pure data transfer laws do not require local storage but only

permit cross border transfers under certain exceptions.

European Laws

The European Union's ("EU") General Data Protection Regulation, together with (a) the United Kingdom's Data Protection Act 2018 and associated post Brexit implementation laws, and (b) implementing laws of EU member states (collectively, "GDPR"), permit transfers of personal data to locations outside of the European Economic Area ("EEA"), which have not been designated as having 'adequate' protections for personal data, only in certain circumstances. Below is an overview of the main mechanisms pursuant to which personal data may be lawfully transferred.

Adequate Safeguards

In the absence of a transfer to a country deemed to have adequate protections for personal data, a controller or processor may transfer personal data outside of the EEA if adequate safeguards are in place and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The GDPR lists a number of appropriate safeguards, the most commonly used being:

1. Binding corporate rules – available only for purposes of intercompany transfers;

2. Standard contractual clauses – currently available for controller to controller, and controller to processor, transfers. Draft updated standard contractual clauses are also under review and would also cover processor to controller, and processor to processor, transfers.

3. Approved certification mechanism (such as the recently invalidated EU / US Privacy Shield framework).

The recent Schrems II decision from the European Court of Justice invalidated the Privacy Shield framework, meaning that personal data could no longer be transferred from the EU to the US under that mechanism. In the same judgment, the European Court of Justice confirmed that Standard Contractual Clauses could still be utilized as a method of transfer, but that in certain circumstances additional safeguards over and above those contained within the clauses would be required. This is particularly applicable to transfers of personal data to the United States, where US government surveillance laws such as FISA 702 mean (at least in the consideration of the European Court of Justice) that enforceable rights and effective legal remedies are not available to data subjects. Recent guidance from the European Data Protection Board has provided further clarity as to the type of additional safeguards that may be required, including data minimization, and encryption of personal data in transit and at rest.

Derogations for Specific Situations

In the absence of an adequacy decision, or appropriate safeguards, a transfer of personal data can still take place pursuant to one of a number of derogations, including:

1. The data subject has explicitly consented to the proposed transfer, after having been informed of the risks of such transfers. It should be noted, however, that there are significant limitations on what is considered valid consent under GDPR, and therefore use of consent for

international transfers should be carefully considered in advance.

2. The transfer is necessary for performance of a contract between the data subject and the controller, or a contract between the controller and a third party where the contract is for the benefit of the data subject.

3. The transfer is necessary for important reasons of public interest recognized under EU or member state law (note, this is usually only applicable in the case of international data exchanges between government authorities and will rarely apply in the context of transfers for business purposes).

4. The transfer is necessary for the establishment, exercise, or defense of legal claims.

5. The transfer is necessary to protect the vital interests of the data subject or other persons, where the data subject is incapable of giving consent. It should be noted that transfers undertaken on the basis of derogations should concern a limited number of data subjects only and may not be repetitive. As a result, reliance on derogations as a mechanism for transfer is appropriate only for occasional transfers and is therefore not a reliable transfer mechanism for most business related transfers (for example, reliance on derogations would not be appropriate for transfers of data to a US based cloud hosting provider, payment processor, or for HR administration purposes).

Laws Outside of the European Union

Below are examples of how various countries outside of the EU have approached data localization and data transfer requirements, and how they fit into the categories of localization/ transfer laws described above.

Broad Localization Laws:

- Russia requires a copy of the data to be stored on local servers, and cross border transfers are permitted under certain exceptions, such as data subject consent.

Specific Localization Laws:

- Japan requires medical care records to be stored within the country.

- China requires certain types of information to be located within mainland China including financial and health or medical information. China’s cybersecurity law also requires certain types of organizations to conduct security assessments prior to transferring personal data outside of China.

- Australia requires certain health information to remain inside of the country.

- India requires licensed banks and payment system providers to retain their information locally and may also be stored additionally outside of India if certain criteria are met.

Combined Localization/Transfer Laws:

- British Columbia and Nova Scotia in Canada both require personal information maintained by “public bodies” (e.g., hospitals) to be stored locally unless the explicit consent to transfer such data outside of Canada and be accessed by nonCanadians is obtained from the data subject.

Pure Data Transfer Laws:

- Brazil restricts the disclosure of personal data outside of the country unless prior consent is obtained, or another exception applies.

- For private entities, Mexico restricts disclosing personal data outside of the country unless notice is given and consent is obtained, or another exception applies. Note that Mexico also has national security provisions applicable to governmental entities that require local storage of national security and public information within the facilities of the relevant public entities.

Conclusion

With the growth of international enterprises, and the ever increasing digital economy, organizations should carefully consider the application of data localization and data transfer laws to their operations and those of their customers. Consideration of these issues as part of product or service development can save time and money and avoid unanticipated legal risk.

National Law Review, Volumess XI, Number 222