大成 DENTONS

Data residency for Canadian companies – The new privacy risk and how to manage it

Thursday, April 8, 2021
12 - 1 p.m. ET (English presentation)
1 - 2 p.m. ET (French presentation)

Your speakers

Chantal Bernier
Counsel
chantal.bernier@dentons.com

Chantal Bernier leads Dentons' Canadian Privacy and Cybersecurity practice group.

She is also a member of the Firm's Government Affairs and Public Policy group.

Chantal advises leading-edge national and international companies as they expand into Canada and Europe, enter the e-commerce space, adopt data analytics and roll out data-based market initiatives.

Her clients include ad tech companies, financial institutions, biotech companies, data analytics firms and government institutions.

Christophe Fichet
Partner
christophe.fichet@dentons.com

Christophe Fichet is partner of the TMT practice in the Paris office.

He has developed a leading sector focus expertise in infrastructures (active/passive) and services dedicated to electronic communications covering France but also the Middle East and Africa, for leading international operators, advisory or investment banks, or international funds like the World Bank.

He also generally advises governments and regulation authorities on the implementation of regulatory frameworks, licensing or privatization processes in several countries.

What is the issue?

- Regulators and consumers are increasingly focusing on the privacy risks related to where personal data is stored:
  - Since July 2020, US organizations have lost the possibility to receive, process and store personal data subject to the GDPR via the agreement concluded between the European Commission and the Federal Trade Commission, meaning the data controllers subject to GDPR can no longer transfer personal data directly or indirectly (including via Canada) to a US receiving organism according to the so called “Privacy Shield”.
  - Cyber-attacks are clearly linked to certain countries – regulators expect Canadian companies to take that into account in choosing service providers
  - Public opinion rises against data storage in countries that do not respect the fundamental right to privacy.

What is the Privacy Risk?

- Regulatory Risk: If you (i) collect and process directly or (ii) receive from partners or customers, personal data subject to the GDPR and store it in the USA, you are facing (i) in the first instance risks of non compliance with regard to GDPR and (ii) in the second case to contractual liability *vis-à-vis* said partners and/or customers, who remain accountable (subject to high sanctions) for data processing and transfer of data subject concerned.
- Security Risk: if you transfer data to countries with little concern for data security, you increase the risk of breach of obligations to protect personal data and to the related accountability principle borne by data controller and to some extent data processor.
- Reputational Risk: If you store data in countries that do not respect privacy, you risk customer churn.

How we will to tackle the issue today:

1. Describing the law on data residency as it applies directly and indirectly to Canadian companies
2. Providing concrete solutions to manage it

What we will not address:

Data residency requirements for public institutions and their service providers

Identifying the Regulatory Risk

- Current:
  - The General Data Protection Regulation (GDPR) maintains the general prohibition for EU companies to transfer personal data outside of Europe, except under some specific and restrictive conditions.
  - Court of Justice of the European Union increased companies' obligations in that regard on July 16, 2020.
  - Guidelines from the OPC and from the OSFI expect organizations to pay particular attention to the factors that may "reduce the foreign service provider's ability" to protect personal information.
- Pending:
  - Quebec Bill 64 proposes requiring a Privacy Impact Assessment before transferring personal data out of Quebec.
  - Canada Bill C-11 (CPPA) formalizes the requirement to inform individuals of the cross-border transfer.
  - Canada is currently negotiating with the EU the right for companies under PIPEDA to receive personal data from the EU.

Data residency under the GDPR

- Article 44 prohibits any data controller or data processor, as defined by the GDPR, from transferring any personal data outside of the EEA, including for onward transfers of personal data from the receiving country, except with “appropriate safeguards” such as:
  - The “importing country” has received adequacy status from the EU Commission for its privacy regime (only 12 countries have “adequacy status”; **OR**,
  - The transfer between companies is subject to EU Commission approved Standard Contractual Clauses (SCC); **OR**,
  - The transfer within a company and its affiliates is subject to approved “Binding Corporate Rules: (BCRs); **OR**,
  - The individual has expressly consented to the cross border data transfer (remote case subject to very restrictive conditions).

What this means for Canadian companies

1. Companies subject to the federal PIPEDA can receive personal data from a data controller (or data processor) subject to GDPR without further authorization because PIPEDA has received “adequacy status”, but they cannot further transfer the data to a country that does not have adequacy status except with SCC, BCR or consent.
2. Companies that come exclusively under provincial privacy law – BC PIPA, Alberta PIPA or Quebec Privacy law cannot receive personal data from the EU except with SCC, BCR or consent because these laws do not have “adequacy status”.
3. The US does not have adequacy status.

What about the EU-US Privacy Shield?

- Gone – invalidated by the decision of the Court of Justice of the European Union (CJEU) of July 16, 2020, commonly called Schrems II
- Why? Because the CJEU deemed US law to allow mass surveillance including of EU citizens without offering them proper redress

SO

- US companies can no longer use certification under the EU-US Privacy Shield to receive personal data subject to the GDPR
- Data controllers and Data processors subject to GDPR can no longer transfer personal data to organizations subject to US laws by referring to the previous Privacy Shield
- Canadian organizations receiving personal data falling within the scope of application of the GDPR must comply with their contractual obligations towards the relevant data controller (or data processor)

The real clincher

- In addition to invalidating the EU-US Privacy Shield, the CJEU
  - Recognizes the validity of SCCs; **but**
  - Requires organizations to strengthen SCCs to ensure their implementation is not undermined in the country of destination.

- This puts the burden of assessing data protection in the country of destination on organizations who are data controllers or data processors according to the GDPR

And what about Brexit?

- February 19, 2021: draft EU Commission decision to grant UK adequacy status

- What is the future of data protection in the UK?
  - Most likely, a gradually more pragmatic application of GDPR
  - See our webinar on GDPR for North American Counsel for more at https://www.dentons.com/en/whats-different-about-dentons/connecting-you-to-talented-lawyers-around-the-globe/events/2021/january/21/gdpr-in-practice-for-north-american-companies

So what do we do now?

- Other available safeguards and derogations to transfer data out of the EU, subject to restrictive conditions

Here are 5 options …

Option #1: Look for service providers storing data in Canada

"*The question is this, as an enterprise, do I have to transfer data to third countries for which there is no adequacy decision by the European Commission? Yes or no? That's the fundamental question*."

Judge von Danwitz, CJEU, (same)

But – storage in Canada may not be practical…

If that is not possible, turn to the “other safeguards” under GDPR

“EU-US Privacy Shield invalidation does not create a legal void because Article 46 safeguards and Article 49 derogations “cover the absence of an adequacy decision”.

Judge von Danwitz, CJEU, Privacy Day speech, January 28, 2021

- So – the data controller (or the data processor if applicable) remains accountable for the re-transfer of personal data subject to the GDPR to service providers located outside Canada.
- Specific commercial contractual obligations according to the quality of the data controller or data processor to be considered, if the Canadian recipient intends to re-transfer the personal data to the USA in particular.

Option #2 : SCCs-Negotiating addenda to current Service Agreements (SA) – Article 46

- New SCCs are about to come out (especially in the case of retransfer from a data processor in Canada to a data processor in the USA).
- Until then, current SCCs are a valid safeguard if they include additional clauses to address EU concern of State access to EU data, such as:
  - Technological measures:
    - Encryption to protect the data from State surveillance
    - End-to-end encryption to argue the data is not “under the control” of the company so the company cannot be compelled to produce
    - “Warrant canary” to alert transferring company of State access request without violating gag orders
  - Organizational measures:
    - Internal policy to challenge all State access requests to personal data subject to the GDPR
    - Data mapping to assess and mitigate specific risk
    - Performing a DPIA or PIA before cross-border transfer
  - Compliance monitoring:
    - Due diligence policy and guidelines in hiring service providers
    - Increased audit rights
    - Duty to consult transferring company in addressing State access request if no gag order

Option #3: VERY RESTRICTIVE option: Incorporate consent to cross border data transfer in consent to service (Article 49)

- Explicit consent of the data subjects may allow (remote and ultimate solution) and subject to very restrictive conditions that shall always be subject to justified reasons, cross border transfer of the data

- Explicit, express and clear consent shall be provided, and may not be bundled as condition to deliver the services or the good.

- Warranties about protection of data concerned in the destination country shall remain required at any moment.

Option #4: Article 49 derogations

- Article 49 creates derogations to the prohibition to cross-border transfer where the transfer is either:
  - Necessary to the contract with the individual
  - In the best interest or to the vital interest of the individual
  - In the public interest
  - Necessary for the defence of legal claims
  - From a register that is meant to be public
- All of these derogations are meant as “one offs” and cannot ground a company’s broad legal approach:
  - If the cross-border transfer is “really required” for the compliance of the contract with the individual, it can be adopted provided:
    - it is not “repetitive”?
    - It applies to a limited number of individuals
    - It is accompanied by suitable safeguards

Option #5: Other Article 46 safeguards

- **Binding Corporate Rules:**
  - Used mostly by multinationals with affiliates around the world e.g. Amex
  - EU Data Protection Authority approved “Binding Corporate Rules” (BCR)
- **Still under development**:
  - Industry associations’ approved code of conduct with binding commitments on data protection
  - Data protection certification mechanisms with binding commitments on data protection

How to choose between the options: Rationalize EU data cross border transfer

- Review data storage location of all service providers
- Perform Transfer Impact Assessment
- On the basis of location of data storage, categorize service providers according to risk:
  - No impact to consider (for e.g. service providers storing all data in Canada or in Europe): no additional contractual measures necessary
  - Impact to consider (for e.g. service provider storing data in the U.S.): negotiating addenda to SA to include strengthened SCCs
  - Significant impact (for e.g. service providers storing data in countries with no existing or effective privacy protection or data security laws): reassessing contracts, negotiating addenda to SA, addressing reality of risk or moving to other service providers

Dentons Roadmap for International Data Transfers – The Transfer Impact Assessment Tool

1. Orientation
   - Internal risk sensitivity and priorisation assessment preparation phase
2. Immediate Risk Solutions
   - Short-term contractual protections and warranties for “in-flight projects” and “emergencies”
3. Data flow/transfer maps
   - Mapping data flows including transfer types, locations and transfer tools in place
   - Assessment of alternative data transfer tools/derogations
4. Local law assessment
   - Standard assessment of local law “gap risk” benchmarked to EU/UK standards
   - Questionnaires for vendors to enhance assessment assurance and/or confirm vendor supplementary measures
5. Assessment phase
   - Assessment of local law/vendor identified risks and definition of required supplementary measures
   - Transfer Impact Assessment (TIA) record, record of mapping, transfer tools assessment and outputs as accountability tool
   - Design of required supplementary technical, organizational and contractual measures
6. Procedural requirements
   - Updating contract warranties and implementing additional policy/technical solutions
7. Re-evaluation
   - Regular process for re-evaluating effectiveness of transfer tools and supplementary measures
8. BAU procurement process
   - Standard vendor diligence processes and procedures for onboarding new/renewal vendors and template contractual updates

Dentons Roadmap for International Data Transfers – The Transfer Impact Assessment Tool

https://www.dentons.com/en/insights/articles/2021/february/2/the-dentons-transfer-impact-assessment-tool

1. Orientation
   - Internal risk sensitivity and prioritization assessment preparation phase
2. Immediate Risk Solutions
   - Short-term contractual protections and warranties for “in-flight projects” and “emergencies”
3. Data flow/transfer maps
   - Mapping data flows including transfer types, locations and transfer tools in place
   - Assessment of alternative data transfer tools/derogations
4. Local law assessment
   - Standard assessment of local law “gap risk” benchmarked to EU/UK standards
   - Questionnaires for vendors to enhance assessment assurance and/or confirm vendor supplementary measures
5. Assessment phase
   - Assessment of local law/vendor identified risks and definition of required supplementary measures
   - Transfer Impact Assessment (TIA) record, record of mapping, transfer tools assessment and outputs as accountability tool
   - Design of required supplementary technical, organizational and contractual measures
6. Procedural requirements
   - Updating contract warranties and implementing additional policy/technical solutions
7. Re-evaluation
   - Regular process for re-evaluating effectiveness of transfer tools and supplementary measures
8. BAU procurement process
   - Standard vendor diligence processes and procedures for onboarding new/renewal vendors and template contractual updates

The upshot for Canadian companies

- If you have the choice to store EU data in Canada – your life will be simpler
- If you do not:
  - Review the location of EU data storage through your service providers
  - Assess the risk for every location/service provider
  - Protect yourself with appropriate contractual clauses
  - Adopt procurement policies to manage cross border transfer risk

Who can help you?

Paris
- Christophe Fichet
  christophe.fichet@dentons.com

Calgary
- Elizabeth Allum
  elizabeth.allum@dentons.com
- Kelly Osaka
  kelly.osaka@dentons.com

Edmonton
- Jaclin Cassios
  jaclin.cassios@dentons.com
- Tom Sides
  tom.sides@dentons.com

Montreal
- Alexandra Quigley
  alexandra.quigley@dentons.com
- Guillaume Savard-Fouquette
  guillaume.savard@dentons.com

Ottawa
- Chantal Bernier
  chantal.bernier@dentons.com
- Charmaine Borg
  Charmaine.borg@dentons.com
- Julia Dales
  julia.dales@dentons.com
- Anca Sattler
  anca.sattler@dentons.com

Toronto
- Luca Lucarini
  luca.lucarini@dentons.com
- Tracy Molino
  tracy.molino@dentons.com
- Karl Schober
  karl.schober@dentons.com
- Chloe Snider
  chloe.snider@dentons.com
- Kirsten Thompson
  kirsten.thompson@dentons.com

Vancouver
- Taylor Buckley
  taylor.buckley@dentons.com
- Facchin, Julie
  julie.facchin@dentons.com
- David Wotherspoon
  david.wotherspoon@dentons.com

Thank you

Chantal Bernier
Counsel
chantal.bernier@dentons.com

Christophe Fichet
Partner
christophe.fichet@dentons.com