The New EU Standard Contractual Clauses

Did you know Dentons produces podcasts on a variety of topics?

Agribusiness

Arbitration

Banking and Finance

Business Insights

Employment and Labour Law

Entertainment and Media Law

Intellectual Property

Life Sciences and Health Care

Mining

Smart Cities

Tax

Transformative Technologies and Data

Women in Leadership and Entrepreneurship

Visit our Podcast page and subscribe: https://www.dentons.com/en/insights/podcasts

Grow | Protect | Operate | Finance

大成 DENTONS

We also have blogs in various areas.

Commercial Litigation

Commercial Real Estate

Drone Regulation

Employment and Labour

Entertainment and Media

Insurance

Mining

Occupational Health and Safety

Privacy and Cybersecurity

Regulatory

Tax Litigation

Technology, New Media and IP Litigation

Transformative Technologies and Data

Venture Technology

Visit our Blogs and Resources page: **https://www.dentons.com/en/insights/blogs-and-resources**

Grow | Protect | Operate | Finance

大成 DENTONS

The New EU Standard Contractual Clauses:

Practical tips for Canadian businesses to use and operationalize the new SCCs

January 26, 2022

Grow | **Protect** | Operate | Finance

大成 DENTONS

Presenters

Chantal Bernier

National Lead of Dentons' Canadian Privacy and Cybersecurity group
D+1 613 783 9684
chantal.bernier@dentons.com

Marc Elshof

Co-Head of Europe Data Privacy and Security group
D+31 20 795 36 09
mark.elshof@dentons.com

Amanda Branch

Senior Associate, Canadian Privacy and Cybersecurity group
D+1 613 288 2713
amanda.branch@dentons.com

26 January 2022

PIPEDA

Canada – Partial Adequacy Status

Decision of adequacy means personal information can flow from the EU to that country without having to implement other mechanisms to protect privacy

Canada has partial adequacy status - an adequate level of protection for personal data transferred from the EU to organizations who are subject to PIPEDA

- PIPEDA applies to private-sector organizations that collect, use or disclose personal information in the course of a commercial activity, also applies to federally-regulated businesses
- PIPEDA does not apply in those provinces with "substantially similar" laws (Alberta, British Columbia and Quebec) - provincial legislation is not deemed “adequate”

When might the transfer of EU personal information to a Canada company require the use of SCCs?

- To organizations not subject to PIPEDA; and
- To organizations that are subject to PIPEDA, but process data outside Canada in a country that does not have adequacy

Data transfers under GDPR

- The GPDR is a walled garden and data can flow freely between EU countries
- For transfers to countries outside the EU additional safeguards must be in place
- This can be done by the European Commission if it rules that a country or territory in a country is “adequate”
- Otherwise, the GDPR has an exhaustive list of “transfer mechanisms”
- The most used of these mechanisms are the Standard Contractual Clauses

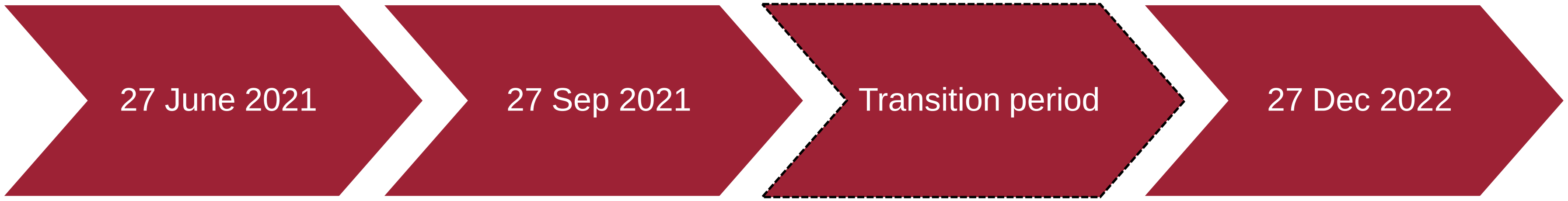
Why new SCCs?

Update for GDPR

More transfers situations

Schrems II

SCCs timeline



27 June 2021

New SCCs become applicable

From this day, the new SCCs can be used for international data transfers.

27 Sep 2021

New SCCs must be used for new transfers

From this day, the new SCCs must be used for new international data transfers.

Transition period

Time to transition to the new SCCs

This transition period allows organizations to transition over to the new SCCs for existing transfers.

27 Dec 2022

New SCCs must be used for all transfers

From this day, the new SCCs must be used for all international data transfers, existing and new.

Extra territorial applicability

Can be used by exporters established outside the EU

SCCs must be passed on down the chain, also outside the EU

Data importer is subject to jurisdiction of EU supervisory authorities

SCCs cannot be used for transfers to non-EU importers ‘subject to’ the GDPR

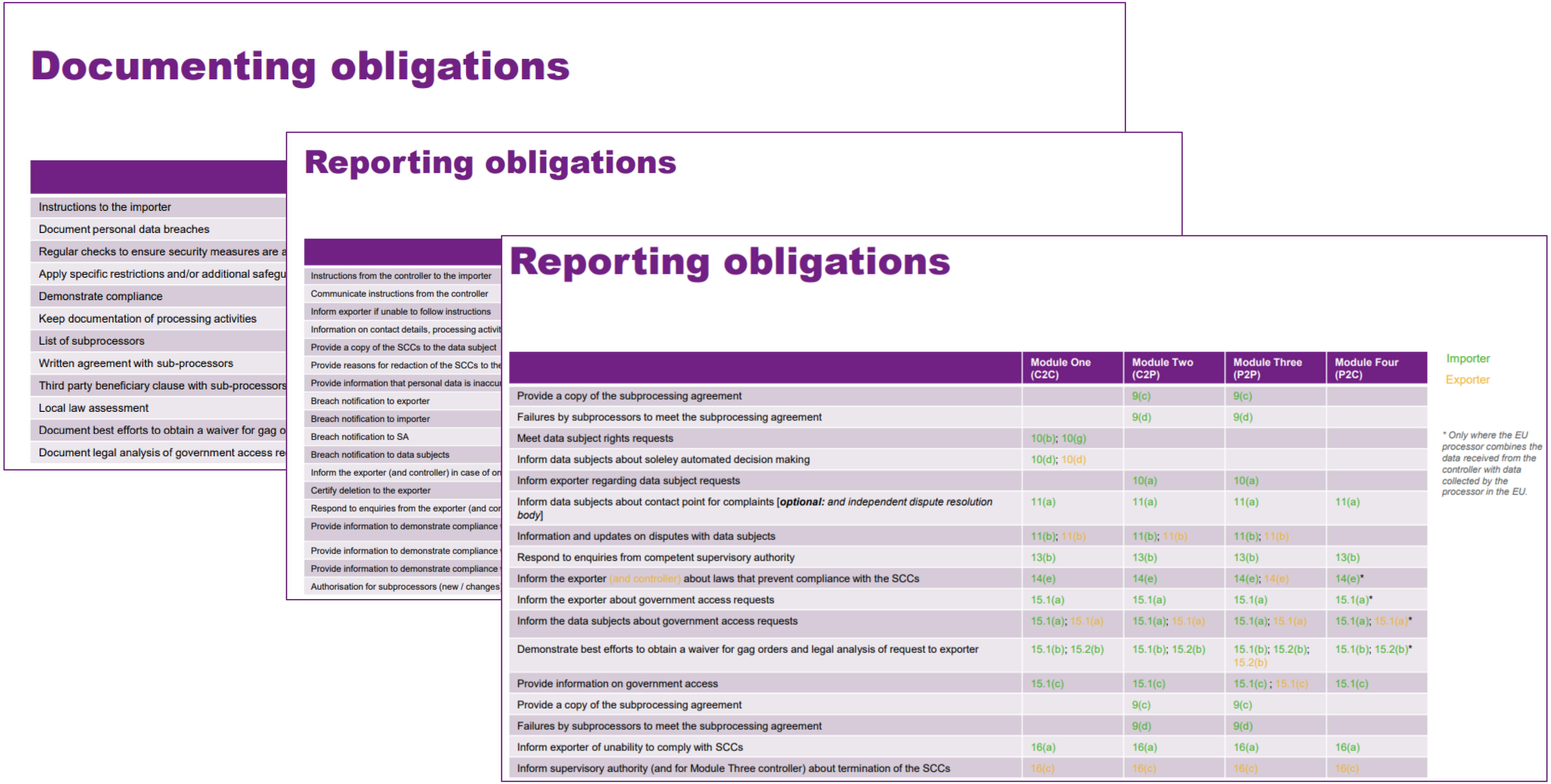
Some key points

Modular approach

Multi-party SCCs

No separate data processing agreement needed (but may be advisable)

Increased reporting and documentation obligations



Documenting obligations

Instructions to the importer
Document personal data breaches
Regular checks to ensure security measures are a
Apply specific restrictions and/or additional safegu
Demonstrate compliance
Keep documentation of processing activities
List of subprocessors
Written agreement with sub-processors
Third party beneficiary clause with sub-processors
Local law assessment
Document best efforts to obtain a waiver for gag o
Document legal analysis of government access re

Reporting obligations

Instructions from the controller to the importer
Communicate instructions from the controller
Inform exporter if unable to follow instructions
Information on contact details, processing activit
Provide a copy of the SCCs to the data subject
Provide reasons for redaction of the SCCs to the
Provide information that personal data is inaccur
Breach notification to exporter
Breach notification to importer
Breach notification to SA
Breach notification to data subjects
Inform the exporter (and controller) in case of on
Certify deletion to the exporter
Respond to enquiries from the exporter (and cor
Provide information to demonstrate compliance
Provide information to demonstrate compliance
Provide information to demonstrate compliance
Authorisation for subprocessors (new / changes)

Reporting obligations

	Module One (C2C)	Module Two (C2P)	Module Three (P2P)	Module Four (P2C)
Provide a copy of the subprocessing agreement		9(c)	9(c)	
Failures by subprocessors to meet the subprocessing agreement		9(d)	9(d)	
Meet data subject rights requests	10(b); 10(g)			
Inform data subjects about soleley automated decision making	10(d); 10(d)			
Inform exporter regarding data subject requests		10(a)	10(a)	
Inform data subjects about contact point for complaints [***optional:*** *and independent dispute resolution body*]	11(a)	11(a)	11(a)	11(a)
Information and updates on disputes with data subjects	11(b); 11(b)	11(b); 11(b)	11(b); 11(b)	
Respond to enquiries from competent supervisory authority	13(b)	13(b)	13(b)	13(b)
Inform the exporter (and controller) about laws that prevent compliance with the SCCs	14(e)	14(e)	14(e); 14(e)	14(e)*
Inform the exporter about government access requests	15.1(a)	15.1(a)	15.1(a)	15.1(a)*
Inform the data subjects about government access requests	15.1(a); 15.1(a)	15.1(a); 15.1(a)	15.1(a); 15.1(a)	15.1(a); 15.1(a)*
Demonstrate best efforts to obtain a waiver for gag orders and legal analysis of request to exporter	15.1(b); 15.2(b)	15.1(b); 15.2(b)	15.1(b); 15.2(b); 15.2(b)	15.1(b); 15.2(b)*
Provide information on government access	15.1(c)	15.1(c)	15.1(c) ; 15.1(c)	15.1(c)
Provide a copy of the subprocessing agreement		9(c)	9(c)	
Failures by subprocessors to meet the subprocessing agreement		9(d)	9(d)	
Inform exporter of unability to comply with SCCs	16(a)	16(a)	16(a)	16(a)
Inform supervisory authority (and for Module Three controller) about termination of the SCCs	16(c)	16(c)	16(c)	16(c)

Importer

Exporter

** Only where the EU processor combines the data received from the controller with data collected by the processor in the EU.*

Putting your SCCs in place in practice

Intra-group agreements

- For Pre-new SCCs intra-group agreements may already use the same modular structure; where possible leverage what you have.
- The group must map the data flows between the various group members to the applicable modules. (Contrast the approach under Binding Corporate Rules to which each group member signs up and which must be approved by the regulator.)
- Supplementary measures, following EDPB guidance, will need to be stated and adopted across all importers or the differences documented.
- The modules require a more detailed description of the transfer than under old rules.
- The new SCCs can be integrated into a broader agreement as long as they are not varied. The broader agreement can accommodate exports from non-EU countries.

External vendors

- For businesses with complex supply chains, consider first assessing the estate, and identifying major exports and principal risks. This aligns with Schrems II concerns and is more practical than starting with a legal analysis.
- Note that the political regime and stability are now fundamental components of the risk assessment (although this is burdensome on private businesses).
- Approach and willingness to cooperate by vendors varies considerably. Raise this topic during the procurement process (Privacy by Design)

Drafting tips

- Start with the annexes, which describe the processing, then choose what measures to apply.
- Differentiate between core immutable measures and "side areas" to be applied flexibly.
- When doing a local law assessment / data transfer impact assessment, focus on local surveillance and government access laws. This is not an adequacy decision and general shortfalls in data protection laws are “remedied” by the use of the SCCs.
- There is no definitive answer as to whether you can limit liability vis-à-vis your contracting party under the SCCs. The European Commission seems to take the position you cannot. However, as this is a commercial arrangement between the parties there is nothing in privacy laws that would prohibit this, provided the data subjects’ rights are not reduced. In specific situations there may be competition law aspects to it (e.g. abuse of market power).

Don’t forget to bring your internal stakeholders on board

This is not a “legal” issue alone.

It affects the business, and you will need engagement from stakeholders:

- Sourcing
- IT (security)
- Marketing / Business Groups
- HR
- C-suite

Without broad support and engagement from the wider organization, you will not be able to achieve substantive compliance

What can we learn from the initial enforcement actions?

Norway: Ferde AS was fined € 496,000 for data transfers to China without proper risk assessment and contractual arrangements.

What can we learn from the initial enforcement actions?

Italy: Bocconi University was fines € 200,000 for data transfers to the US because there was insufficient information provision to the data subjects, and the contractual arrangements were outdated (still based on Privacy Shield).

What can we learn from the initial enforcement actions?

Portugal: The National Institute for Statistics was ordered to suspend its transfers to the US or other third countries until a Transer Impact Assessment was done and supplementary measures implemented.

What can we learn from the initial enforcement actions?

Germany: A company was ordered to stop using Mailchimp because of the associated transfer of data to the US

What can we learn from the initial enforcement actions?

Austria: Austrian SA ruled that the use of Google Analytics violates the GDPR

大成 DENTONS

Thank you

Chantal Bernier
National Lead of Dentons' Canadian Privacy and Cybersecurity group
D+1 613 783 9684
chantal.bernier@dentons.com

Marc Elshof
Co-Head of Europe Data Privacy and Security group
D+31 20 795 36 09
mark.elshof@dentons.com

Amanda Branch
Senior Associate, Canadian Privacy and Cybersecurity group
D+1 613 288 2713
amanda.branch@dentons.com

26 January 2022

大成 DENTONS

What’s Next? The answer is Talent.

With more than 20,000 people, 12,000 lawyers and 200 locations, Dentons has the talent for what you need, where you need it.