PRIVACY AND DATA UPDATE

Trading internationally? The new EU data protection SCCs explained

SHOOSMITHS

Your hosts

Connect with your hosts on LinkedIn by scanning the QR codes below.

Sarah Tedstone, Partner
Sarah.Tedstone@shoosmiths.co.uk
+44 (0) 756 295 0800
+44 (0) 121 625 4277

Hamish Corner, Partner
Hamish.corner@shoosmiths.co.uk
+44 (0) 773 370 7674
+44 (0) 207 205 7011

Today's session

An update on how to keep your data flowing internationally

Presenters:

Sarah Tedstone and Hamish Corner

23 June 2021

SHOOSMITHS

Trading internationally: quick recap

Safeguards may be needed for international personal data transfers depending on the locations involved

List of countries deemed already adequate by the EU and UK and not needing safeguards: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. UK decision awaited

BCRs are the gold standard

Privacy Shield was critical for EU-US transfers

SCCs are EU-approved template terms which ensure GDPR standards are met provided the terms are respected. We previously had two sets of approved SCCs for data transfers in limited circumstances from data controllers in the EU to data controllers outside the EEA and for data controllers in the EU to data processors outside the EEA which pre-dated the GDPR and which were practically unworkable.

Standard Contractual Clauses (SCCs)

Privacy Shield

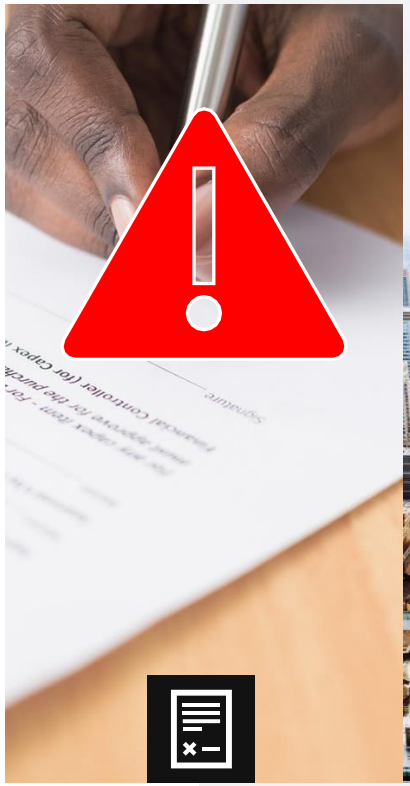
Binding Corporate Rules (BCRs)

What was the Schrems 2.0 case about?

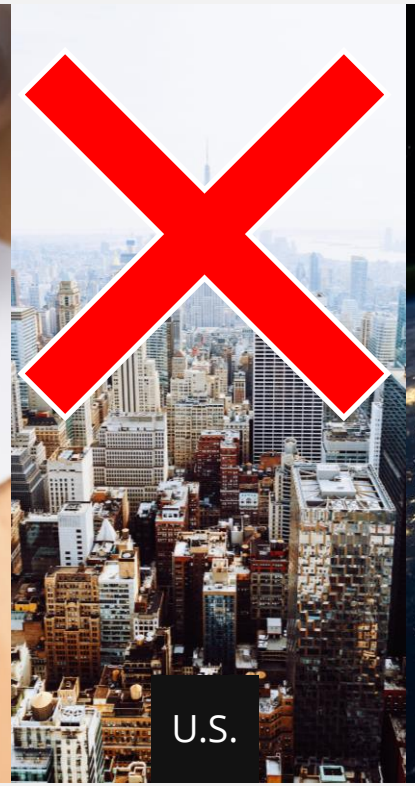
The case was principally about whether the Privacy Shield and existing SCCs offered enough protection:

- *The Privacy Shield was invalidated with effect from 16th July 2020 because of U.S. surveillance activities and there being no actionable rights for EU/EEA citizens*
- *The existing SCCs were seen to be technically valid, but it was made clear they are not a paper or tick box exercise. Organisations on both sides must do an assessment of whether there is equivalence with EU law and either not transfer or terminate the contract if necessary. We have called this exercise "SCC+" since the Schrems 2.0 decision. The new SCCs and guidance give clarity on these aspects*
- *BCRs remain a key safeguard*

"protection granted to personal data in the EEA must travel with the data wherever it goes"



Standard Contractual Clauses (SCCs)



Privacy Shield

Binding Corporate Rules (BCRs)

What next? Brexit Are new safeguards needed?

Check

- Do you transfer personal data from the EU/EEA to the UK? Check your records of processing activities/ data maps

New requirements

- Reportedly EU governments have approved the UKs Adequacy decision set to be in place by 30 June meaning safeguards will not be needed for EU-UK transfers
- The new SCCs will need UK approval for use and are not valid for restricted transfers from the UK in the meantime. The existing SCCs must be used
- New UK SCCs are expected within weeks

UK Representative

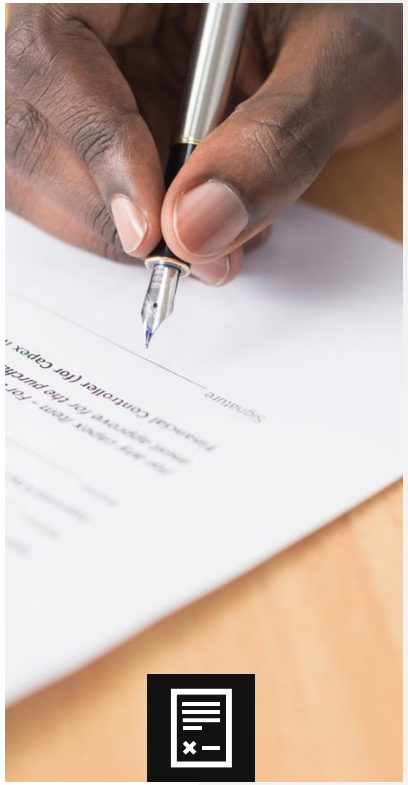
- From 1 January 2021, those companies who do not have a physical footprint in the UK but who sell to or monitor people in the UK must appoint a UK representative-see Shoosmiths' fixed price, online service which offers this service at our dedicated webpage at https://www.shoosmiths.co.uk/dataprivacyrep

SCCs: the new versions and guidance: pros and cons

New final SCCs were published on 7 June 2021 which are very similar to the draft versions

New final guidance is now available, more is expected

SCCs for international transfers are often used when transferring personal data to countries and territories which are not on this list of countries deemed already adequate: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay

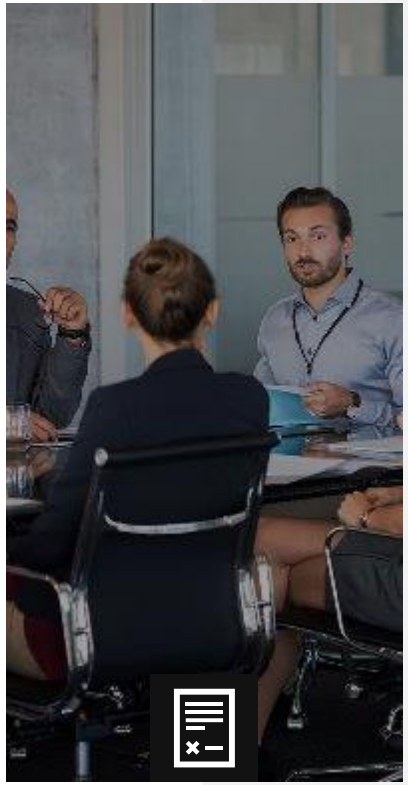


Standard Contractual Clauses (SCCs)

- Now modular multi-party possibilities to cover combinations of four scenarios:
  - controller-controller
  - controller-processor
  - processor-processor
  - processor to controller
- Suitable for data exporters not located within the EU but caught by the GDPR terms.
- Processor mandatory terms under Art 28
- Schrems 2.0 risks covered
- **Time periods: 27 September 2021 for all new contacts and amendments. 27 December 2022 for all existing contracts**
- Wider responsibilities to understand the chain of processing from the ultimate controller to the last sub-processor
- Tougher notification requirements to parties in the processing chain and EU data protection authorities
- They involve creating a contract from relevant choices and an assessment of wider risks and laws involved. Inserting them by reference into a contract will no longer be possible
- Data protection authorities are expected to 'up their game' on enforcement and there are indications that this is happening
- We are seeing stakeholders take a much keener interest in the detail as we predicted in July 2020
- The parties give warranties that they have no reason to believe that local laws and practices in the data importer's country prevent compliance. There is now additional guidance about this
- The EU guidance has further clarified the SCC+ assessment exercise. Understand the SCC obligations. They require significant vigilance, legal advice, ongoing monitoring and action
- There are also new SCCs for controller to processor contracts generally giving some certainty about these common terms

International SCCs: creating your contract

Think SCC +



Standard Contractual Clauses (SCCs)

- Creating your contract from relevant choices:
  - Standard clauses that apply in all scenarios:
    - Enforcement of rights by data subjects and dealing with complaints by both parties
    - Liability, indemnity, identifying the competent supervisory authority and jurisdiction (data importers always liable to data subjects for damage they cause)
    - Dealing with law enforcement requests and local law conflicts
    - Process if data importer becomes unable to comply
    - List of parties, description of transfer, technical and organizational measures and list of sub-processors
    - Both parties to consider security including during transmission
    - The SCCs have priority over other contracts and terms should not contradict them
  - Optional clauses
    - A docking clause: new parties can be added later
    - Modules for the four scenarios: controller to controller, controller to processor, processor to processor and processor to controller
    - Minor aspects of some modules eg approval of sub-processors

International SCCs: creating your contract

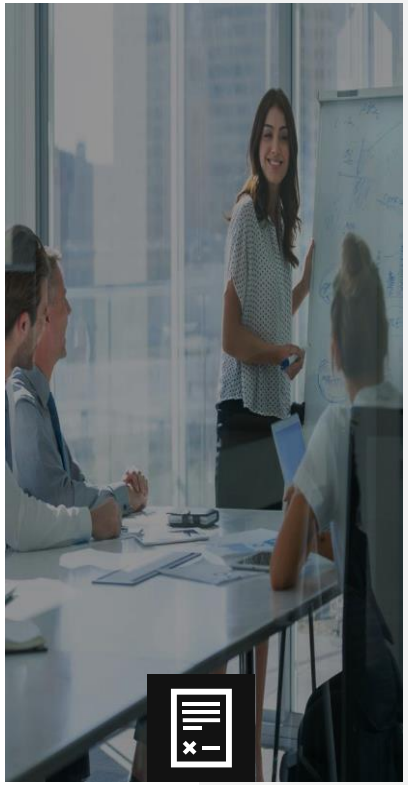
Think SCC +

Standard Contractual Clauses (SCCs)

- Module 1: controller to controller
- Data importer:
- Limited purposes
- Provide certain privacy information to data subjects
- Obligation to action rectification and erasure and deal with other data subjects' rights
- Data minimization and storage limitation
- Without undue delay notify any breach to data exporter and competent supervisory authority if breach likely to create a risk to data subjects and if there is a high risk also notify data subjects
- Ensure onward transfers have safeguards and on its instructions
- Restrictions on special category data
- Both:
- Security obligations and agreed details to be included
- Module 2: controller to processor
- Data importer:
- Typical GDPR controller to processor clauses
- Follow data exporter's instructions including for onward transfers and notify if cannot
- May have to demonstrate compliance to competent supervisory authorities
- Data exporter:
- To exclusively control key for pseudonymized data

International SCCs: creating your contract

Think SCC +



Standard Contractual Clauses (SCCs)

- Module 3: processor to processor
- Data importer:
- Process on documented instructions from controller and additional instructions from data exporter which must not conflict
- Notify data exporter if cannot comply
- Notify data exporter and where appropriate and feasible the controller of breach and data subjects' rights
- Only disclose to a third party on documented instructions from the controller
- Demonstrate compliance to data exporter, controller and competent supervisory authority
- Restrictions on special category data
- Audits from data exporter and controller
- Typical GDPR controller to processor clauses flowed down
- Restrictions on sub-processing
- Data exporter:
- Inform data importer that it acts as processor under instructions of controller which will be provided prior to processing
- Inform controller if data importer cannot follow controller's instructions
- Exclusively control key for pseudonymised data (or the controller)
- Impose same obligations on importer as controller has imposed on it

International SCCs: creating your contract

Think SCC +

Standard Contractual Clauses (SCCs)

- Module 4: processor to controller
- Data importer:
- Refrain from any action that prevents data exporter from complying with GDPR

- Data exporter:
- Only process on documented instructions of data importer acting as its controller
- Notify data importer if cannot follow data importer controller's instructions
- Extra obligations if it *combines the personal data received from the data importer with personal data collected by the data exporter in the EU especially regarding access by public authorities*

- Both:
- Cooperation to respond to the exercising of data subjects' rights

International SCCs: your obligations pre-transfer

Think SCC +

Standard Contractual Clauses (SCCs)

Understand the obligations within the SCCs you are signing and the wider (EDPB) guidance

- Know your transfers:
  - by reference to Record of Processing Activities (RoPA)
  - map out your locations
  - what is a transfer? includes remote access from a third country (eg support), and/or cloud storage outside EEA
  - remember onward transfers by others of the data entrusted to them. i.e. all actors in the chain
- Keep in mind data minimisation
- Data exporter to assess the third country protections & if data importer can satisfy its obligations:
  - must be documented. Might need to produce to the competent data protection authority
  - are supplementary clauses / safeguards needed
  - If the GDPR level of protection is undermined, or the supplementary measures are prohibited or contradict the SCCs, you should not start, or suspend, and consult
- Re-evaluate at regular intervals

International SCCs: your obligations pre-transfer

Think SCC +

"You should conduct this assessment with due diligence and document it thoroughly, as you will be held accountable to the decision you may take on that basis"

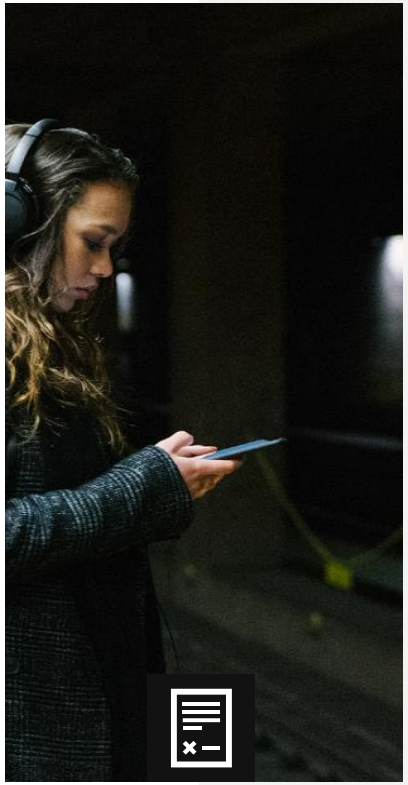
Standard Contractual Clauses (SCCs)

Transfer Risk Assessments - factors to be considered from the SCCs and EDPB guidance:

- must be documented
- nature and purposes of the transfer (marketing, HR, IT support, storage and Sector in which the transfer occurs (health, financial) and categories of personal data
- any processors or sub-processors involved
- types of entities involved in the processing (public/private, controller/processor)
- whether the data will be stored in the third country or if there is only remote access
- format of the data to be transferred (pseudonymised, encrypted)
- possibility of onward transfers
- if data subject rights can continue to be effectively applied
- If a right of redress for data subjects in case of access to their data by public authorities in the third country
- effective limits on surveillance requests and publicity about the location

International SCCs: your obligations pre-transfer

Think SCC +



Standard Contractual Clauses (SCCs)

What do the new SCC clauses and guidance say about local laws and public authority/government surveillance requests?

- Both parties warrant that they have no reason to believe that laws of third country prevent the data importer's ability to comply with SCCs
- *When reviewing local laws, the parties can take account of how laws are interpreted or applied in practice. e.g. documented previous experience of requests or the experience of others in the industry, and similar transfers. Must be a robust assessment, corroborated by relevant, objective elements.*
- Data importer warrants it has made best efforts to provide data exporter with relevant information and will continue to cooperate to ensure compliance
- Data importer must notify the data exporter if it becomes unable to comply. The data exporter must identify additional safeguards to address situation, or if not possible must suspend data transfer. Data exporter may terminate contract in that event
- Data importer must (if permissible/possible) notify data exporter and affected data subject(s), if a disclosure request / order etc is received from public authorities or courts of third country, or if it discovers those authorities are obtaining direct access to personal data. The data importer must review and document the legality of the request and challenge it if there are reasonable grounds to consider it unlawful.

International SCCs: your obligations pre-transfer

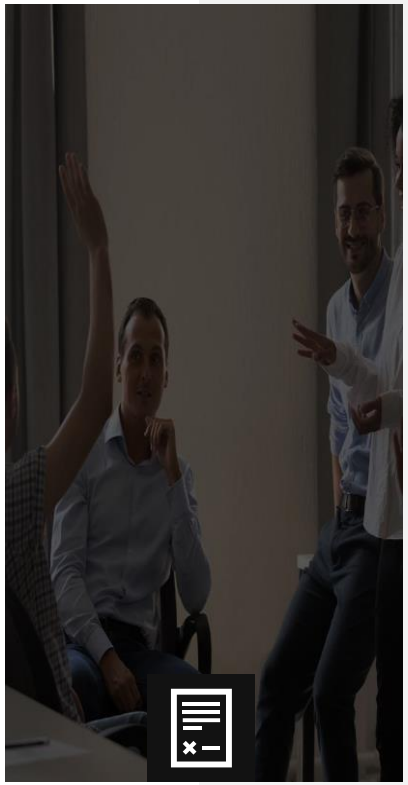
Think SCC +

Standard Contractual Clauses (SCCs)

- Supplementary measures in addition to using the SCCs:
- Technical
  - Encryption
  - Pseudonymisation
  - Split or multi-party processing
- Additional contractual measures
  - Eg specifying the technical measures needed
  - Eg contract annexes for the importer to provide about investigation into surveillance access, and that encryption keys do not have to be handed over
  - Reinforced audit clauses
- Organisational measures
  - Internal policies, methods and best practices
  - Records of surveillance requests
  - Data minimisation

International SCCs: your obligations ongoing

Think SCC +



Standard Contractual Clauses (SCCs)

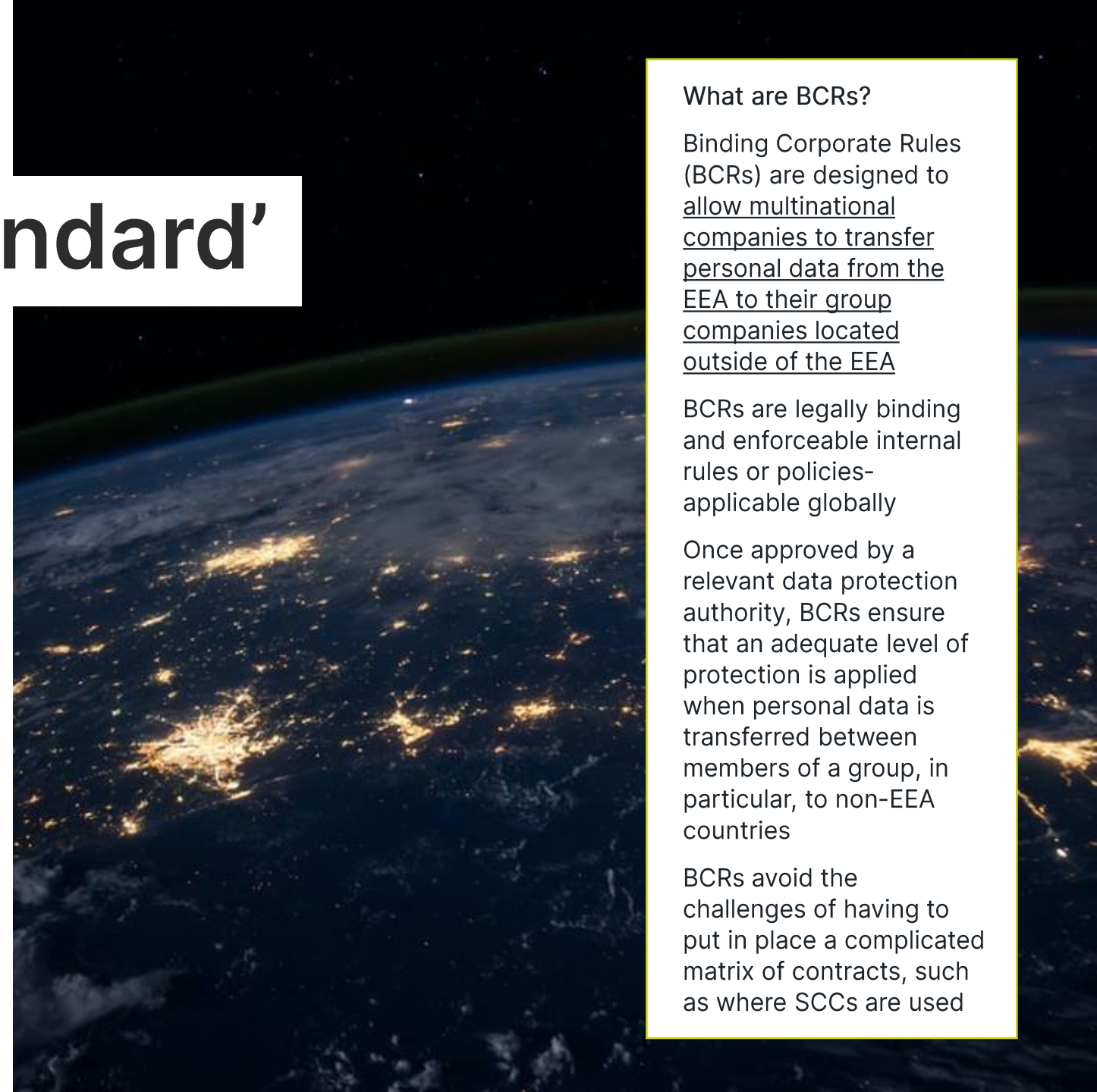
- Understand the obligations within the SCCs you are signing and the wider guidance
- Monitor ongoing developments in the third country/your location
- Keep track of changing instructions in the services
- Storage limitation- keep track of contract durations, retention periods, obligations to return or delete
- Be aware of restrictions and confidentiality obligations for employee access
- Third party sharing may be prohibited, or if not keeping track of sub-processors will be needed and contracts to be disclosed
- Data importer has certain duties to notify not just the data exporter but the ultimate controller and competent supervisory authority
- Keep track of data protection authority assessments of risky locations

BCRs: the ‘gold standard’

Check
- Are BCRs sensible for your business? For smaller businesses they are unlikely to be feasible (Hybrid DTAs are a good alternative). For multinationals they are by far the safest option

Review your privacy program
- Are you doing what you have committed to doing?
- How is your program doing generally?

Apply for BCRs
- Application offers regulatory protection (NB you are not irrevocably committed)



What are BCRs?

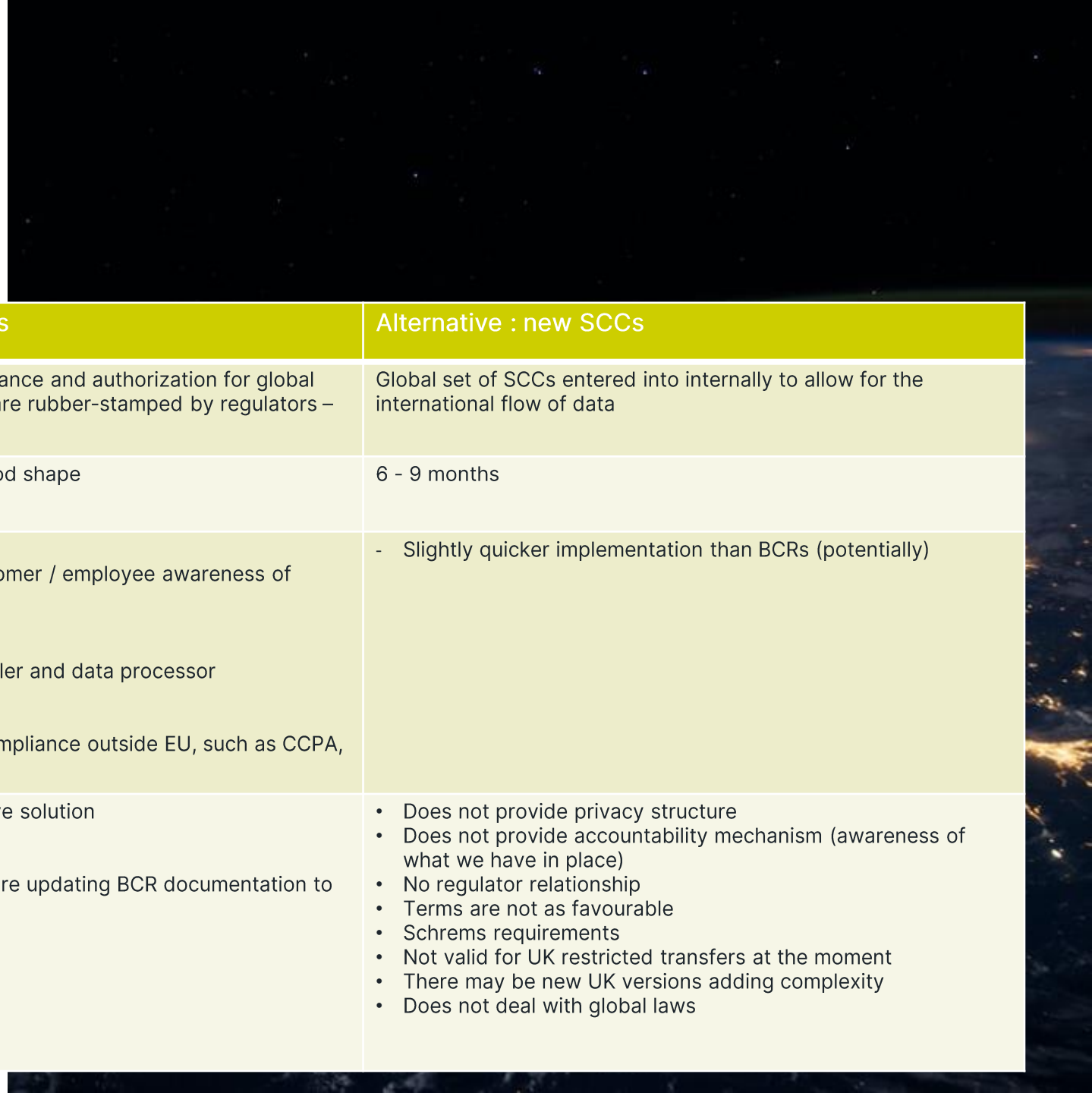
Binding Corporate Rules (BCRs) are designed to allow multinational companies to transfer personal data from the EEA to their group companies located outside of the EEA

BCRs are legally binding and enforceable internal rules or policies- applicable globally

Once approved by a relevant data protection authority, BCRs ensure that an adequate level of protection is applied when personal data is transferred between members of a group, in particular, to non-EEA countries

BCRs avoid the challenges of having to put in place a complicated matrix of contracts, such as where SCCs are used

BCRs v SCCs



Executive summary

Subject	Proposed solution: Binding Corporate Rules	Alternative : new SCCs
Content	Global set of GDPR policies and procedures, governance and authorization for global data transfer which binds all company entities and are rubber-stamped by regulators – shows accountability to the outside world	Global set of SCCs entered into internally to allow for the international flow of data
Timing	9 -12 months, if GDPR compliance in reasonably good shape	6 - 9 months
Pros	- Globally recognized and on your website - Provides privacy and security structure and customer / employee awareness of compliance - Speeds up customer and vendor negotiations - Regulator approval and relationship - Applies to both company acting as a data controller and data processor - Provides accountability under GDPR - Regulatory future-proofing - Accommodates other global privacy laws and compliance outside EU, such as CCPA, Turkey, India, Brazil and most of Asia	- Slightly quicker implementation than BCRs (potentially)
Cons	• Takes slightly longer to implement than alternative solution • Will have to have an operation in mainland EU • May need to apply for UK BCRs too • EDPB still expect compliance with Schrems and are updating BCR documentation to allow for that • Some external contracts may still be needed	• Does not provide privacy structure • Does not provide accountability mechanism (awareness of what we have in place) • No regulator relationship • Terms are not as favourable • Schrems requirements • Not valid for UK restricted transfers at the moment • There may be new UK versions adding complexity • Does not deal with global laws

Conclusions and practical next steps

- Safeguards possible
- Medium to large companies:
    - BCRs controller and processor which address processing internally and with customers
    - Hybrid DTA, and
    - SCC+ (including transfer risk assessments)
- Smaller companies:
    - Hybrid DTA, and
    - SCC+ (including transfer risk assessments)
    - Watch out for UK approval of the new SCCs and new UK SCCs

Conclusions and practical next steps

- By 27 September 2021:
    - Understand your data flows and locations involved
    - Assess what safeguards are needed, urgently if that was previously the Privacy Shield or after 30 June 2021 Brexit if the UK is not deemed adequate. BCRs? SCCs?
    - Watch UK position
    - For all new international contracts needing SCCs or for changes to such existing contracts and data flows undertake SCC+:

- By 27 December 2022 all existing SCC contracts will need redoing using SCC+

- What is SCC+?:
    - Create your modular SCC contract choices applicable to each flow
    - Undertake your transfer risk assessments
    - Implement any supplementary measures (such as contract terms, technical and organisational measures) for risky locations
    - Understand your obligations in the new SCCs
    - Due diligence with commercial partners
    - Watch out for warnings about other countries being unsafe

    Ensure you're not just undertaking paper compliance: amendments to policies and privacy notices will be needed

Conclusions and practical next steps

Shoosmiths support

- Automated Privacy Compliance digital tools
    - In partnership with OneTrust
    - Modular including data mapping
    - Significant discounts available
    - 90 day free trial
- SCC+
    - Our tried and trusted model
- UK and EU Representatives
    - https://www.shoosmiths.co.uk/dataprivacyrep

Watch out for these webinars as things develop:

- Brexit and Data Protection: the Finale?
  July 2021 (depending on UK adequacy decision)
- Global privacy program: practical tips
  August/September 2021

Any questions?

Your hosts

Connect with your hosts on LinkedIn by scanning the QR codes below.

Sarah Tedstone, Partner
Sarah.Tedstone@shoosmiths.co.uk
+44 (0) 756 295 0800
+44 (0) 121 625 4277

Hamish Corner, Partner
Hamish.corner@shoosmiths.co.uk
+44 (0) 773 370 7674
+44 (0) 207 205 7011

WEBINAR

Thank you

Visit our events page:
https://www.shoosmiths.co.uk/insights/events

SHOOSMITHS