



TaylorWessing

Data Protection Webinar

The new standard contractual clauses

What does this mean for data transfers?

17 June 2021

Private and confidential

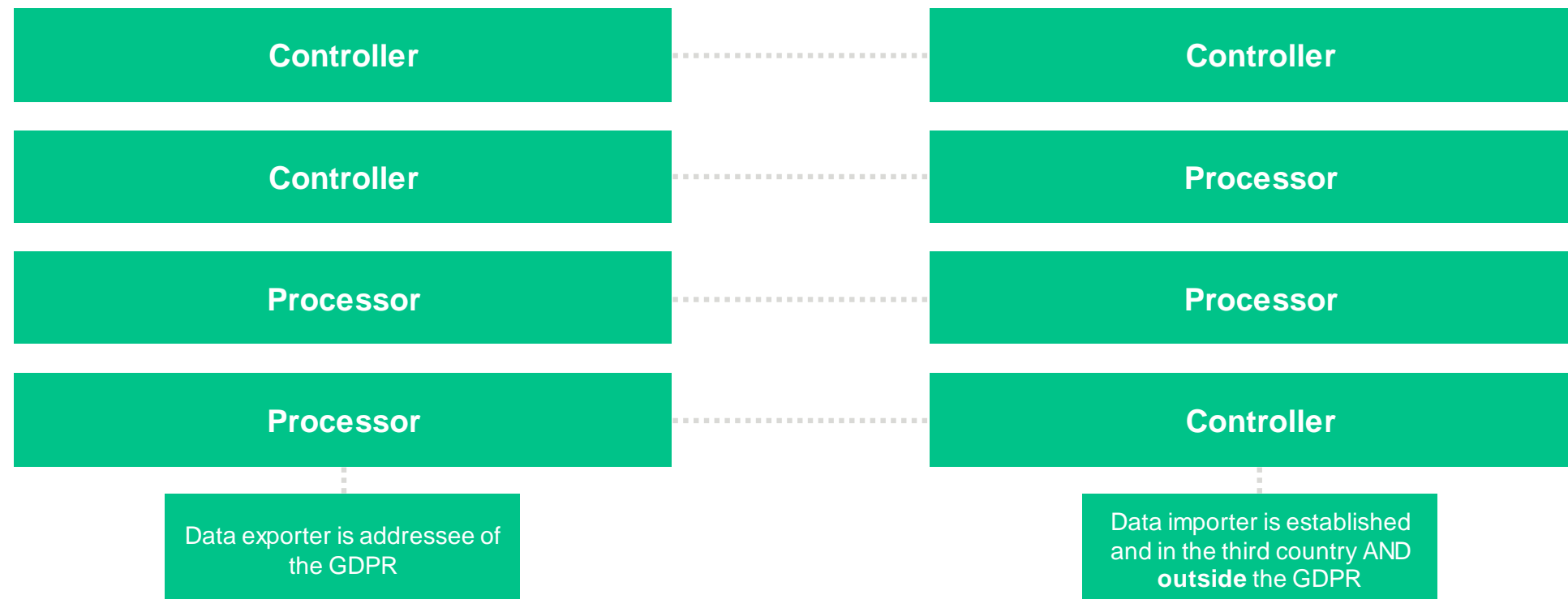
New standard contractual clauses

Overview

- Publication in the Official Journal of the European Union **on 7 June**
- **Which means**
 - **As of 27 September 2021:** new SCCs must be **used** on any new transfer (or existing transfer when processing operations changed)
 - **As of 27 December 2022:** updating **all existing** SCCs to the new SCCs, as the 'old' SCCs C2P and C2C are repealed then.

New standard contractual clauses

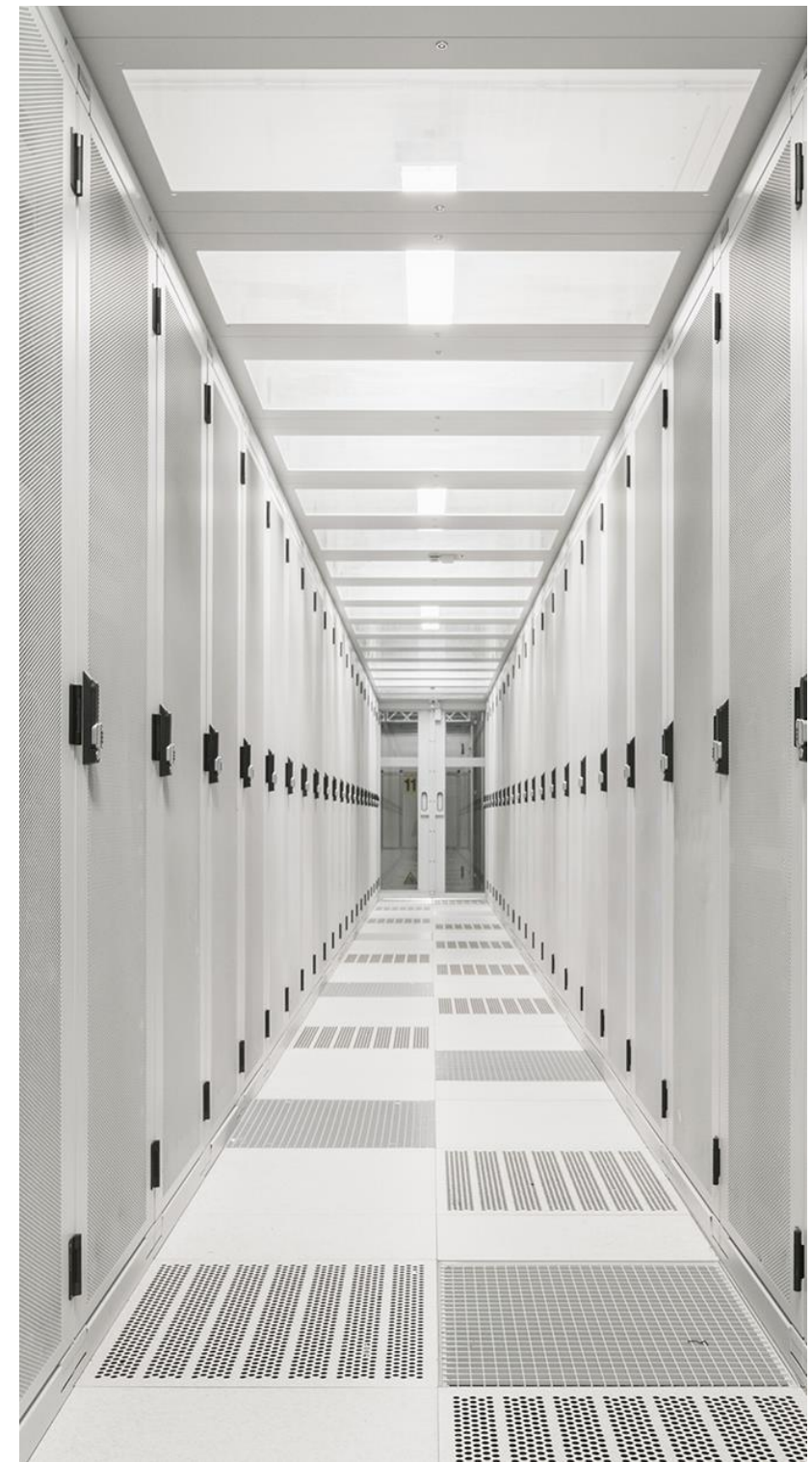
Constellations and scope of application



New standard contractual clauses

Introduction

- No additional agreement under Art. 28 (3) GDPR required for C2P and P2P (unless some processing in EEA)
- Inclusion of the constellation Processor-to-Processor (long awaited)
- P2C – obstacle of competition for EU processors?
- Multi-party possibilities for both data importers and exporters
- Choice of law and jurisdiction within the EU



New standard contractual clauses

Relevance with regard to the *Schrems II* judgement

- The parties' warrant for the level of protection in the third country*
- Transparency/information obligations*
- Obligation to examine official requests for data disclosure*
- Obligation to minimise data when replying to a request for disclosure*
- Exhaustion of the legal remedy in the context of the defence against official requests for disclosure
- Documentation obligations

* Some of the EDPB's recommendations already taken into account



New standard contractual clauses

Schrems II

Transfer Impact Assessment, clause 14

- Assessment of third-country laws and practices on data protection standard
- Risk-orientated approach?
- Obligation to document and to provide on request

Obligations in case of access by public authorities, clause 15

- Notification of the data exporter and, where possible, the data subject promptly
- Review of legality of the request and judicial action when chance of success
- Documentation of legal assessment and any challenge to the request
- Data minimisation when responding

New standard contractual clauses

Other

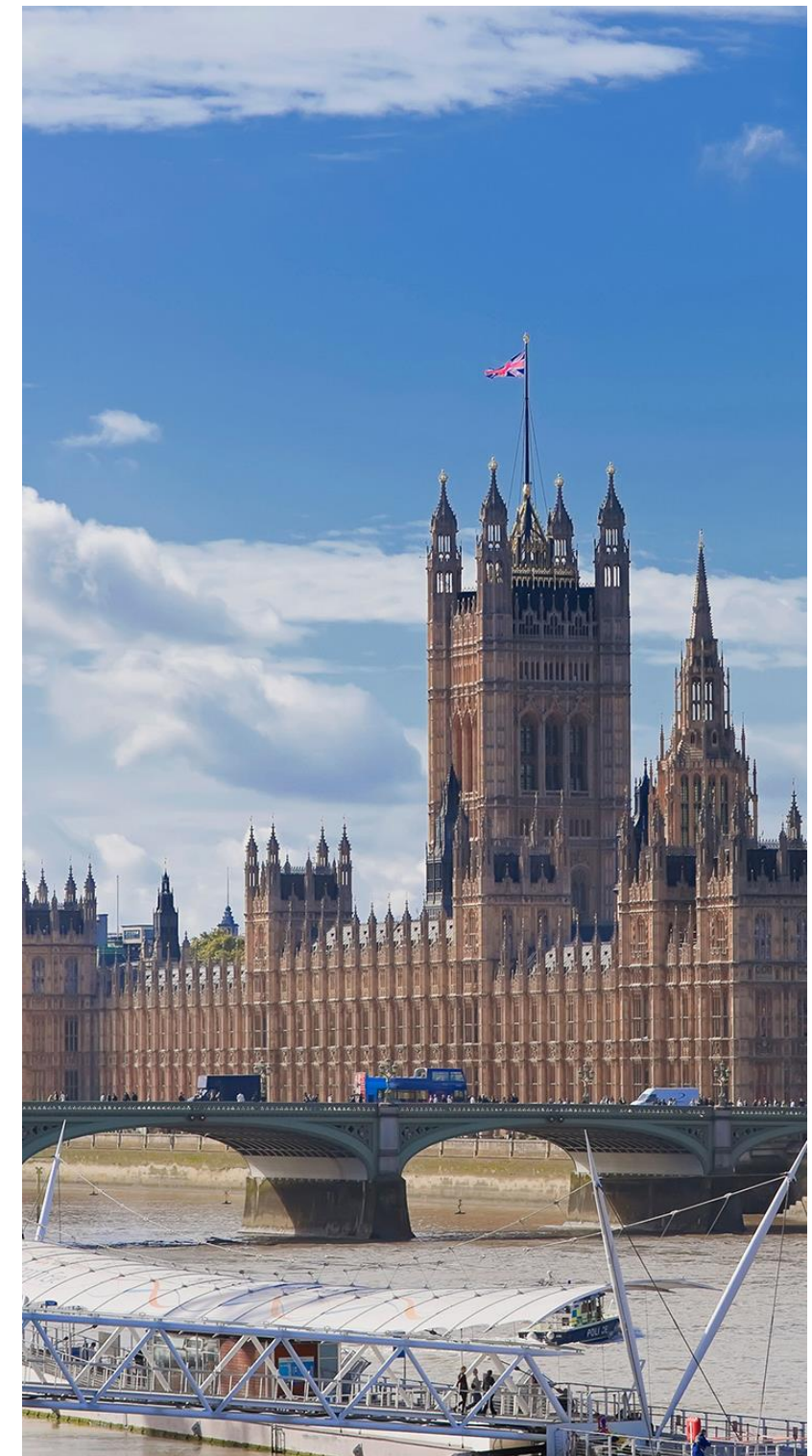
- a) Fixed character
- b) Third-party preference
- c) Hierarchy
- d) Liability
 - For data importers harder to limit their liability
- e) Docking Clause
- f) Supervision
- g) Choice of law and jurisdiction
 - For module 4 even of third-country
- h) More, including
 - Obligation to make available a copy of the SCC to people affected
 - Documentation of measures taken
 - Special termination rights for breaches
 - Specific rules on legal remedies

Initial thoughts/expectations

- Some good stuff: modular, processor-to-processor, flex to use fold into MSA or other contract documents.
- EU customers likely to start asking before September, especially as the new SCCs present an (incomplete) answer to Schrems II concerns
- So US vendors do not have much time to get their own templates together
- Article 28 DPA also published – don't forget that, EU customers likely to push for it too for processing in the EEA
- Flex to embody the new SCCs in an MSA, DPA or as own standalone document. Either way still a "sacred text" which cannot be amended.
- We expect US vendors to try to 'float on top' provisions managing audit and sub-processor notifications as they do at present.

Quick word about the UK & Switzerland

- New EU SCCs not valid under UK or (yet?) under Swiss law
- UK will issue own new SCCs but not clear when or how similar
- Hoped that ICO will in practice accept that combined UK and EU transfers are OK under new SCCs, but not clear – risk need to carry on using both
- For now, old SCCs work for Switzerland too but not the new ones – expected that the Swiss regulator will adopt the new ones but tbc



Pain points & operationalisation

- Third country assessments and information under clause 15? What should vendor-importers provide to EU customers? Full DTIA, or list of countries and country assessments?
- What does reporting to exporters on LEA requests at regular intervals mean – how exactly do we operationalise? Has to be consistent.
- Audit rights – rights to information and audit at reasonable intervals and where indications of non-compliance – vendor certifications *may be taken into account and may include inspections at premises or physical facilities*
- Put a framework around when physical attendance can happen at their premises and clarify that third party data centres out of scope? NB tough to justify that just the SOC 11/ ISO reports enough.
- Sub-processors – options around specific consent or general authorization and objection process for new sub-processors, processors to give enough information to assess – specific notification?
- Security measures – annex as before but driving for more detail than we are used to – InfoSec team

What to do?

- Game-plan –complicated project: contract amendment and operationalisation – internal & external resources, and comms internally – will be a long process
- Data-Mapping – including which module fits where
- “Customizing” the SCC
- Process of transfer impact assessment
- Switch to the new SCC (**3-months** and **18-months** period after publication)
- Documentation and constant re-evaluation of taken measures
- **Any questions?**

Who we are

Taylor Wessing is a global law firm that serves the world's most innovative people and businesses.

Deeply embedded within our sectors, we work closely together with our clients to crack complex problems, enabling ideas and aspirations to thrive.

Together we challenge expectation and create extraordinary results.

1000+ lawyers | 300+ partners | 28 offices | 16 jurisdictions



International data protection practice

Taylor Wessing advises on all areas of data protection across all sectors. As businesses strive to create more value from data, and find even more creative ways of interacting with customers, the various laws that govern use of data and protection of information touch more businesses.

We regularly advise businesses on issues such as:

- Implementing national and international corporate data protection policies, structures and departments
- GDPR audits and implementation
- Risk remediation
- Data protection and data security Data protection issues in transactions


International data protection practice (cont'd)

- Worldwide roll out of contracts
- Employee data protection (e.g. implementation of HR database)
- Assessment of new processes and IT systems (e.g. HR or CRM systems)
- Advising companies in audits of regulatory authorities and in potential disclosure or summary proceedings
- Authorization concepts
- International data protection requirements (SCC, BCR, Privacy Shield, ad hoc contracts, opt-ins)
- Advising on the introduction of new products and services (preliminary evaluation).

Global Data Hub

The Global Data Hub is Taylor Wessing's international thought leadership in the area of data protection. The Global Data Hub draws on the firm's international expertise to provide you with insight and practical guidance on the data protection issues most likely to affect your organisation. www.taylorwessing.com/globaldatahub

Latest articles




June 2018

Data breaches and enforcement – what can we expect under GDPR?

Paul Glass reads between the lines on fines.

[Read more](#)




June 2018

Protecting corporate reputation following a data breach

Michael Yates looks at reputation management the wake of a GDPR data breach.

[Read more](#)


Data Privacy tools



EEA Personal Data Transfer tool

Use our checklists to help ensure you comply with the GDPR and put the right procedures and priorities in place.


[VISIT TOOL](#)



HR GDPR Assessment tool

This free assessment tool identifies key areas of GDPR risk focussing on the employee data environment by using a streamlined question flow approach.

[VISIT TOOL](#)




Global Data Protection Guide

The Guide spans more than 60 countries and takes the form of an interactive online map, which clients can use to compare national data protection laws in multiple jurisdictions.

[VISIT GUIDE](#)


Hot topics



GDPR

The GDPR is a complete overhaul of EU data protection law. Compliance is an ongoing obligation which you must be able to demonstrate. Get to grips with the most pressing GDPR issues.


[VIEW MORE](#)



GDPR checklists

Use our checklists to help ensure you comply with the GDPR and put the right procedures and priorities in place.

[VIEW MORE](#)



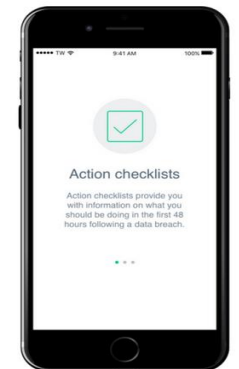
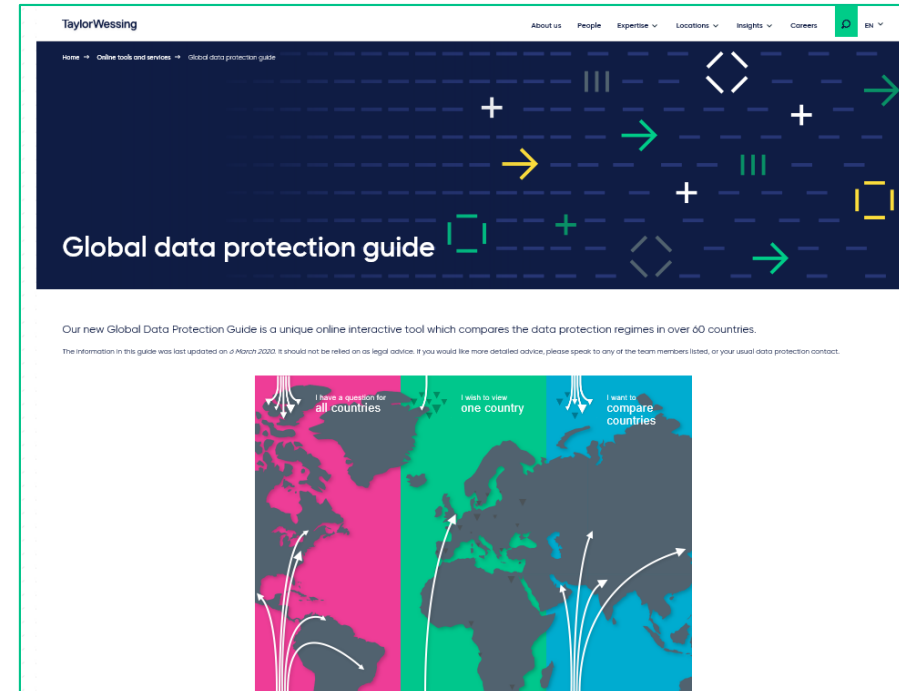
Cybersecurity

Getting cybersecurity wrong can lead to reputational damage, financial loss and damaging litigation. Using our Global Data Hub resources can help you get cybersecurity right.

[VIEW MORE](#)

Global Data Protection Guide

- Cyber-attacks are on the increase. It is estimated that 68% of all large businesses, and 52% of small businesses, have fallen victim to a security attack in the last year. Yet only 29% of companies have a formal cybersecurity policy in place and just 13% of businesses set security standards for suppliers or contractors to adhere to. When the GDPR comes into effect in May 2018, companies face potential multi-million pound fines for data breaches.
- TW: Cyber Response has been developed and designed to help companies respond quickly and effectively should a breach occur. In essence, it provides companies with practical assistance to help them minimise their exposure to regulatory action, litigation risk and reputational damage should a breach occur
- The app is available from the Apple App Store and the Google Play Store.



Our Global Data Protection Guide looks at the data protection regimes in over 60 countries across the world. Data Protection is a core business issue for all companies in all sectors at the moment and this product helps to demonstrate to clients that we are always thinking about their business needs.

Legal Tech Services | SCC Generator

One Tool for all new SCCs: Our SCC Generator will help you to determine the right set of Standard Contractual Clauses (SCC) in accordance with the European Commission's Decisions 2021/914 and 2021/915 from 4 June 2021.

The Generator is capable to assemble the comprehensive SCC template for the following processing situations:

Art. 28 (7) GDPR Template	Templates for Third Country Transfers
Controller to Processor	Controller to Controller
	Controller to Processor
	Processor to Processor
	Processor to Controller

Our SCC Generator will guide you with questions through the process and will provide you with the relevant contract template that includes the clauses applying to your processing situation.

After answering a few questions, you can download a suitable template in DOC format.

Your Contact



Dr. David Klein
Salary Partner, Hamburg

d.klein@taylorwessing.com



Benjamin Stach
Senior Associate, Hamburg

b.stach@taylorwessing.com



scc@taylorwessing.com

Your Taylor Wessing team

Axel von dem Bussche is a specialist lawyer for information technology law. He heads up the Technology, Media & Telecoms practice group and coordinates Taylor Wessing's international US Group for Germany.

With his considerable years of experience and outstanding expertise, he routinely guides clients from the technology sector through complex international transactions, contract drafting and regulatory issues. Axel is an accomplished data protection and GDPR expert. He supports corporate groups with the transformation to digital and global business models and also conducts negotiations with the responsible regulatory authorities.



Data protection specialist Axel von dem Bussche advises well-known clients on data issues (...). He also represents clients in proceedings on a regional and national level against data protection supervisory authorities.

Chambers & Partners Europe 2021



Frequently recommended for information technology, data protection and media

**“one of the best, absolute strategist” ;
“absolute expert in the industry”**

JUVE 2015/2016-2020/2021



**Dr. Axel Frhr. von dem Bussche,
LL.M. (L.S.E.)**

Partner, Hamburg

+49 40 36803-229

a.bussche@taylorwessing.com

Key areas of expertise

- IT & Telecoms
- Data Protection
- Copyright & Media Law
- Litigation & Dispute Resolution
- Technology, Media & Communications

Languages:

- German, English, French

Your Taylor Wessing team

Vinod Bange is the head of our UK data protection and privacy team.

Vin specialises in data protection and information law, working with clients from various data-rich sectors including retail, financial services, life sciences, healthcare, and technology.

He has over 15 years of experience and is known by his clients for giving advice that is insightful, commercial and explained without necessary jargon.



The practice is led by Vinod Bange, whose extensive, specialist knowledge shines through his pragmatic, commercial and client-oriented advice.

Legal 500



Vinod Bange

Partner, London

+44 20 7300 4600

v.bange@taylorwessing.com

Key areas of expertise

- Data Protection
- Information Law
- Data Security
- Technology Supply and Procurement
- Technology Regulatory Compliance

Your Taylor Wessing team

Chris is a seasoned data protection and technology partner and specialises in supporting multi-national technology companies and online platforms.

Chris guides clients through complex contractual negotiations, Platform to Business Regulation, digital advertising, global data protection governance and compliance, and all areas of doing business online.

His clients span the digital advertising, fintech, eCommerce, mobile, enterprise software, enterprise SaaS and high-end engineering sectors.

Clients praise Chris's practical and commercially-minded advice.



Christopher Jeffrey

Partner, London

+44 207 300 4230

c.jeffery@taylorwessing.com

Key areas of expertise

- Data Protection
- Information Law
- Data Security

Your Taylor Wessing team

Paul Voigt specialises in IT and data protection law. He advises clients on national and international data protection projects, and has proven expertise in IT contract and security law as well as e-commerce.

In four languages - German, English, French, Spanish - he advises companies of all kinds: from newly founded start-ups to medium-sized companies and global players. In addition, Paul represents online gambling providers in civil and administrative proceedings right up to the Federal Administrative Court. He also regularly assists overseas clients on their market entry in Europe.

Numerous publications and recommendations are a testament to Paul's expertise.



Paul Voigt combines an almost inexhaustible specialist knowledge with an equally large economic understanding

Legal 500



Frequently recommended for Data Protection and IT law

"super and fast lawyer", "extensive competence", "restless, deserves to be a partner", "business-oriented, Rising Star", "good in topics with IT security law implications"

JUVE Directory 2020/2021



Paul Voigt, Lic. en Derecho

Partner, Berlin

+49 30 885636-410

p.voigt@taylorwessing.com


Key areas of expertise

- Data Protection
- IT & Telecoms
- Copyright & Media Law
- Litigation & Dispute Resolution

Languages:

- German, English, Spanish, French

1000+ lawyers 300+ partners 28 offices 16 jurisdictions



Austria	Klagenfurt Vienna	Poland	Warsaw
Belgium	Brussels	Slovakia	Bratislava
China	Beijing Hong Kong Shanghai	South Korea	Seoul*
Czech Republic	Brno Prague	UAE	Dubai
France	Paris	Ukraine	Kyiv
Germany	Berlin Düsseldorf Frankfurt Hamburg Munich	United Kingdom	Cambridge Liverpool London London TechFocus
Hungary	Budapest	USA	New York Silicon Valley
Netherlands	Amsterdam Eindhoven		

* In association with DR & AJU LLC

© Taylor Wessing LLP 2021

This publication is not intended to constitute legal advice. Taylor Wessing entities operate under one brand but are legally distinct, either being or affiliated to a member of Taylor Wessing Verein. Taylor Wessing Verein does not itself provide services. Further information can be found on our regulatory page at:

www.taylorwessing.com

TaylorWessing



SCC 2021 Updates

*Program
Management &
Operational
Support*

SENTINEL

Now that the new SCCs are out...what now?

Each organization will need to assess all transfers of personal data out of the EU and the related contractual relationships.

This work will include updating existing contracts using the old version of SCCs with the new SCCs, and if any contracts still leverage Privacy Shield, replacing those with another approved mechanism.



How can we help

We have developed and delivered a methodology to help rapidly respond to the near-term problems of:

- Assessing international data transfers & transfer mechanisms
- Identifying & reviewing existing vendor contracts
- Project managing the complex process of getting contracts updated.

Our approach helps organizations future-proof their vendor management process and applicable systems in anticipation of additional changes to privacy requirements that will likely occur in future.

Clients will see the immediate impact of this methodology and our reliable project accelerators, freeing up their team to deliver core privacy outcomes.

Operational guidance

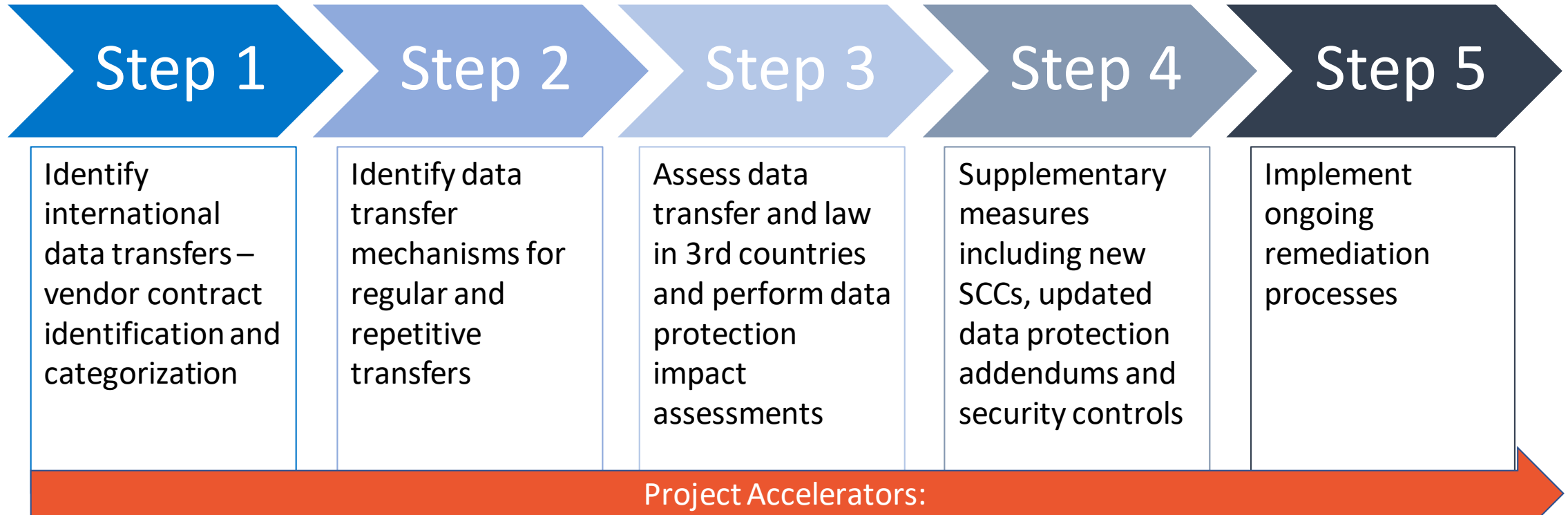
Our approach helps organizations:

- Understand where personal data is transferred
- Re-evaluate the level of protection for data transferred to third countries at appropriate intervals
- Implement supplementary measures and tools to ensure data transfers are permissible in the absence of an EEA/EU adequacy decision.
- Ensure that internal and external stakeholders are engaged throughout the process.
- Leverage tracking and project management systems to keep the project on track.



Phased approach and project accelerators

Aligned with EDPB guidance, providing comfort for internal stakeholders and regulators



Project accelerators will facilitate a fast and efficient engagement to meet the EU Commission's 18-month deadline:

- Reliable knowledge of the contractual data required
- Efficient vendor outreach process
- Optimized tracking system
- Well developed and tested standard operating procedures
- Executive reporting dashboards
- Effective contract templates



Combines people, process and technology to assess, implement and operate effective privacy programs that drive business value



**Strategic
Program Design**



**Privacy Program
Management
Office support**



**Readiness
Assessments &
Roadmaps**



**Program
Measurement
and Metrics**

**Comprehensive Privacy Program
Management with Ethos™ Platform**



Clients	Services provided in 2021
Fortune 25 Technology company	Privacy Messaging and Strategic support
Fortune 50 Retailer	Privacy Program Management Office
Fortune 50 Technology company	Privacy Research
Fortune 75 Technology company	Strategic Privacy Support
Fortune 75 Technology company	Privacy Training
Fortune 100 Manufacturer / retailer	Ethos Privacy software platform and related services
Fortune 300 Technology company	Strategic Privacy Support & Privacy Engineering
Fortune 500 Technology company	Strategic Privacy Support and Program Management Office



Aaron Weller

FIP, CIPP/US, CIPT, CIPM

President, Sentinel

aaron@sentinelcsg.com

cultureofprivacy.com



SENTINEL