Luther.

First-aid kit for “Schrems II” compliance

After the European Court of Justice (ECJ) declared the EU-US Privacy Shield invalid in “Schrems II”, businesses are now facing the question of how to deal with this judgment. The decision has already now a significant impact on the assessment of data transfers outside the EU/EEA, in particular to the USA, under data protection law. International data transfers can no longer be justified by reference to the Privacy Shield. But also standard data protection clauses, even though they are valid, must be viewed increasingly critically. Some data protection supervisory authorities are of the opinion that such clauses can no longer be readily used to justify international data transfers. And there is no prospect of a quick fix for this problem, as the critical aspects relate mostly to the terms and conditions of the Privacy Shield and the legal situation prevailing in the USA.

This is why businesses should examine their data transfers, inter alia those to the USA and to other third countries that do not ensure an adequate level of protection (e.g. China, Russia, and the Middle East), and take additional measures to provide for an adequate level of data protection. Where sufficient measures cannot be taken, exit strategies might be required depending on the circumstances. To avoid such potentially serious consequences, and until the data protection supervisory authorities have provided concrete help, the package of provisional measures set out below can be used to evaluate data transfers and identify and address any risks that may exist:

Step 1

- Identifying international data transfers and the third-country service providers used
- Differentiating between US Privacy Shield and standard data protection clauses
- Categorising the respective data transfer based on the amount of risk involved using the self-assessment checklist (see below)

Step 2

- Examining the existing agreements and the measures taken
- Vendor due diligence: asking the data importers about safeguards and their risk assessment (in particular, whether the data importer is able to comply with its obligations arising from the standard data protection clauses)

Step 3

- Implementing **additional** technical and organisational measures, e.g. enhanced encryption
- Implementing and/or agreeing **additional** obligations/ safeguards (obligations to furnish information, supplements to the standard data protection clauses)

Step 4

- Examining alternatives that can be used to justify international data transfers (for instance, binding corporate rules (BCR), extended consent regarding cookies, for example)
- Documentation and evaluation

Step 5

- First package of measures to protect international data transfers
- Ensuring that evidence exists which can be presented to the data protection supervisory authorities (this reduces the risk of conditions and administrative fines being imposed)
- In general: overview of international data transfers and risks, proof of compliance
- Decision-making basis for risk assessments and exit strategies
- Optimising the processes for commissioning and regularly monitoring the service providers employed

Self-assessment checklist - risk assessment of international data transfers after Schrems II

Risk factors (examples)

Factors/measures increasing the risk	Risk factor “target country”	Impact on risk*
	Critical third country, such as the USA, China, Russia, or the Middle East (possibly also the UK in the future)	
	Special risks regarding government access based on national security acts (e.g. FISA 702, EO 12333)	
	Limited legal protection for EU data subjects	
	Risk factor “service provider/data importer”	
	Provider of telecommunications services	
	Provider of electronic communications services (e-mail, video, Messenger, etc.)	
	Cloud provider	
	Service provider/data importer was already in the past an addressee of measures regarding access by the government	
	Analysis/tracking services provider (e.g. website tracking)	
	Provider of secondary IT services (maintenance, support, etc.)	
	Intra-group data transfer/service provider	
	Risk factor “type of data”	
	Special categories of personal data (health, religion, etc.)	
	Sensitive bank and financial data	
	HR data	
	Inventory data of employees or end-customers (contact details, e-mail address, user name)	
	Usage data (log-in data, web-tracking data, without localisation)	

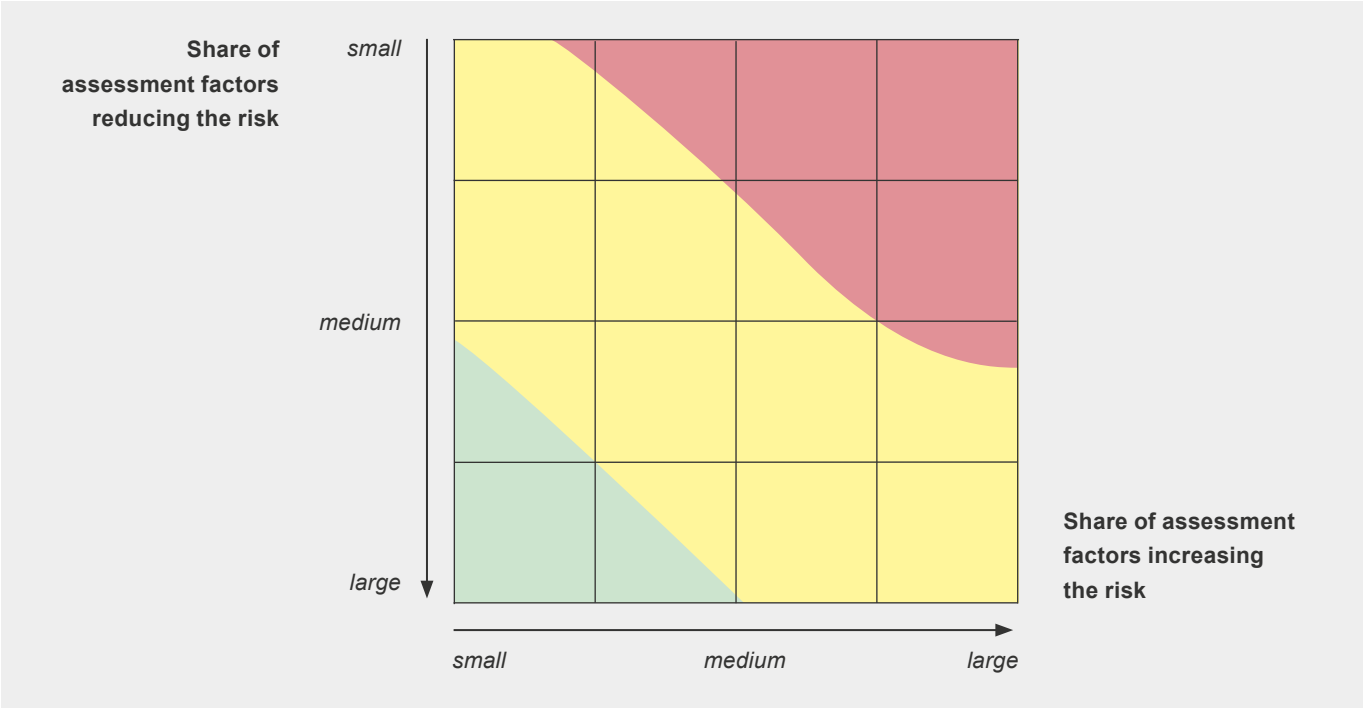
Factors/measures reducing the risk	
	Standard data protection clauses with extended obligations/security measures, in particular, transparent information and, where applicable, approval by data exporter in the event of access by public authorities
	Extending the rights of data subjects/compensating for deficits in legal protection
	Compliance confirmation from service provider
	Certification of service provider regarding data protection/data security
	Involving the data subjects – consent solution
	Binding corporate rules (BCR)
	Codes of conduct
	Limitation to pseudonymous data/tokenisation
	Data localisation EU/EEA (container solution, trustee model)
	Encryption measures
	Other technical or organisational security measures to restrict access

* “Impact on risk” key	- increases the risk -	- risk-neutral - Risk exists, but is not increased	- reduces the risk -

The impacts on risk will be classified on a best practices basis without liability.

Evaluation matrix - categorising the risk potential

This matrix can be used to compare the established risk factors with the measures reducing the risk and to determine the risk potential for the respective international data transfer. On this basis, further measures can then be determined, if necessary, depending on the risk classification.



Risk category 1	Risk category 2	Risk category 3
Exit strategy/alternative to transferring data to a third country	Using standard data protection clauses following adjustments can be justified	Using standard data protection clauses is generally safe

Your contacts

Dr Michael Rath
Lawyer, Partner
Certified specialist in IT law
Cologne
T +49 152 016 25745
michael.rath@
luther-lawfirm.com

Silvia C. Bauer
Lawyer, Partner
Cologne
T +49 221 9937 25789
silvia.c.bauer@
luther-lawfirm.com

Dr Stefanie Hellmich, LL.M.
Lawyer, Partner
Frankfurt a.M.
T +49 69 27229 24118
stefanie.hellmich@
luther-lawfirm.com

Christian Kuß, LL.M.
Lawyer, Partner
Cologne
T +49 221 9937 25686
christian.kuss@
luther-lawfirm.com