



US SAFE HARBOR FRAMEWORK DECLARED INVALID

How to continue legally transferring personal data to the United States

Summary of the ruling

October 6, 2015, in a ground-breaking judgment, the Court of Justice of the European Union declared the US Safe Harbor framework to be invalid, and confirmed that individuals have the right to challenge any similar adequacy decisions that may be established by the European Commission through their national data protection authorities.

The US Safe Harbor framework was established 15 years ago to provide a mechanism by which European businesses could validly transfer personal data from the EU to the US. The framework has been widely adopted, with over 4,500 companies using the framework to support the free flow of data across the Atlantic. It is commonly adopted for data transfers needed to support intra-group operations (for example to assist a US parent in managing EU-based activities) and outsourced services involving a US cloud or software-as-a-service provider.

The decision of the Court will have a significant and immediate impact for any business relying on Safe Harbor to legitimize transfers and will require a change in approach to cross-border data flows.

1. The ruling of the European Court of Justice affects far more than US tech companies.

- It affects any company relying on Safe Harbor as a legal basis for transferring user, customer, employee or any other personal data to the United States, either intra-group or through the supply chain.

2. Impact on past transatlantic data flows with Safe Harbor as (sole) legal basis

- Data flows prior to the Court ruling are still considered to be compliant. The legality of the current processing in the US of those earlier transferred data remains unclear.

3. Impact on ongoing, real time transatlantic data flows with Safe Harbor as (sole) legal basis

- The Court ruling does not order an immediate end to such personal data flows, but national Data Protection Authorities (DPAs) have the right to suspend such transfers if they do not provide sufficient privacy protections.
- The immediate consequence of the Court ruling is that the Safe Harbor decision is invalid and thus it is likely that personal data flows under the framework will be challenged by national DPAs.
- If a local DPA suspends transatlantic data flows that are supported only by the Safe Harbor, future transfers would be in violation of European data protection laws if no other valid legal basis for transfer exists.
- If a local DPA suspends transatlantic data flows for this reason, further "onward transfers" of personal data would likewise be in violation of European data protection laws absent another valid legal basis for transfer.
- Organisations should realise that other arrangements on personal data transfers may also be challenged in the future, such as the so-called model clauses and "white-country" adequacy decisions.



4. Preliminary reaction from DPAs and EU institutions

- There are 28 Member States and more than 28 DPAs, which creates the risk of fragmentation of approaches when data flows to the US originate from multiple Member States. Nonetheless, the European Commission and some DPAs immediately voiced in the days following the ruling that they want to move forward uniformly for the sake of providing legal certainty across the EU.
- A common position and guidance of the European Commission as well as the Article 29 Working Party (assembling the national DPAs of the 28 EU Member States) is expected starting the week of 12 October.

Foreseeable consequences if you don't act now

- breach of contracts and exposure to damages and/or triggering of termination rights
- user/customer/employee complaints made with the controller (or processor)
- user/customer/employee complaints to the DPA
- orders and injunctions of DPAs
- loss of potential new business in Europe

WHAT DO YOU NEED TO DO NEXT?

STEP 1. Map your data flows

Especially for organizations with complex cross-border data flows due to their group structure or variety of outsourced (data processing) operations, it is strongly advised to map the cross-border data flows, to **understand** in which scenarios personal data is transferred from the EU to the US.

- ☑ Such mapping exercise will allow to **prioritize** the key data transfers (from an operational and risk perspective).
- ☑ Such exercise will include **reviewing** the contracts you have in place with your vendors who process personal data on your behalf, to verify whether these vendors process EU personal data in the US, or process EU personal data in the EU but have a contractually stipulated right to relocate the data (e.g., in a cloud context). This also includes reviewing your contracts in terms of subcontractors. Data transfers

from vendors to their subcontractors must include the same rights and must also ensure an adequate level of protection.

- ☑ Use of EU-based servers and systems which are frequently **accessed** from the US will also qualify as a transatlantic data transfer and will thus also require a legal basis to legitimize the transfer.

STEP 2. Patch your transatlantic data transfers within the same group of companies

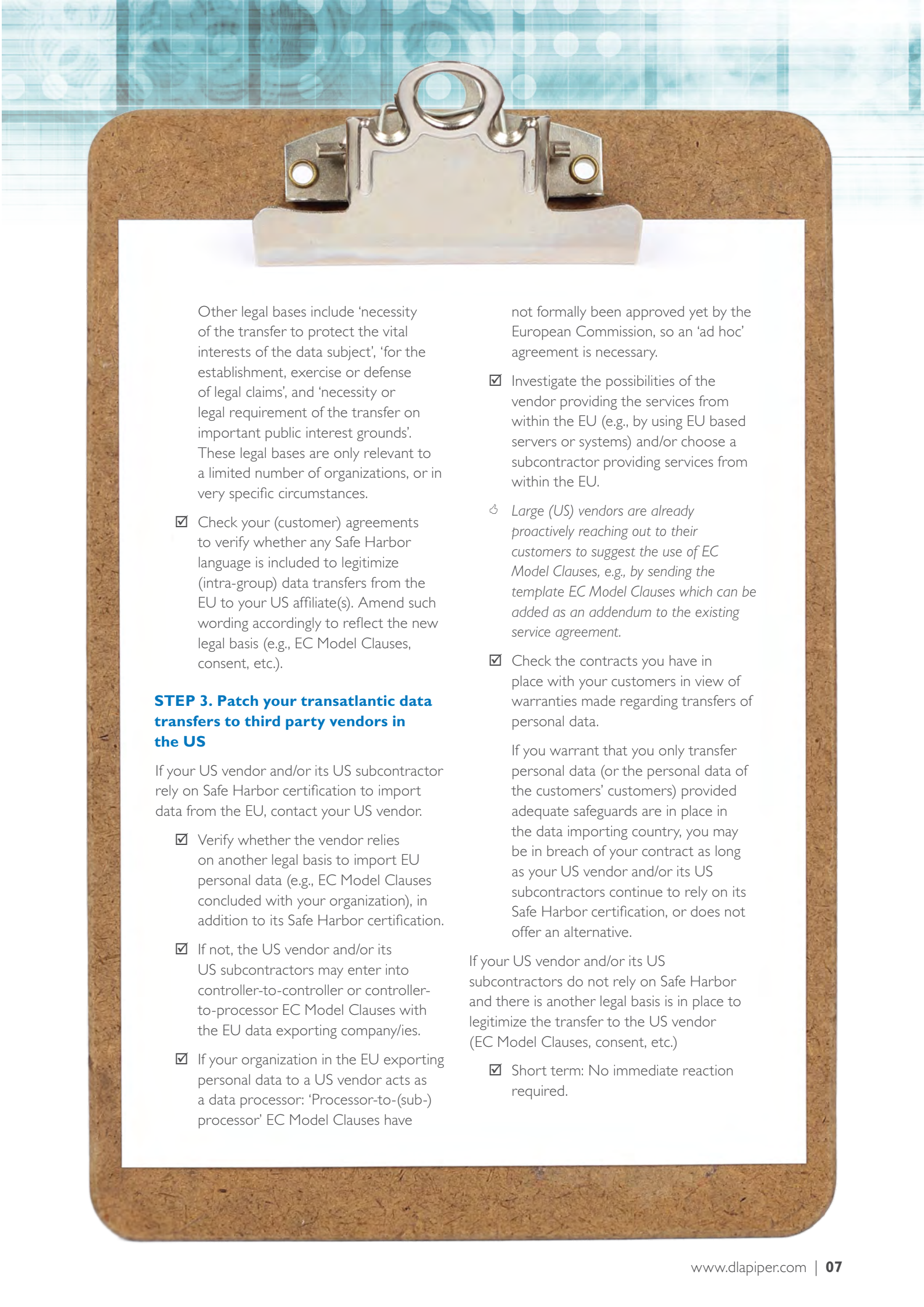
If you are based in the EU and are relying on the Safe Harbor certification of the 'data importing' US affiliate as a sole legal basis to legitimize intra-group data transfers:

- ☑ Note that Safe Harbor is no longer valid as a legal basis for transfers from the EU to the US.
- ☑ Put in place another legal basis:



Legal basis	Pros	Cons
European Commission (EC) Model Clauses	<p>Quick and efficient</p> <p>Standard template</p> <p>May be used in relation to third parties which are not members of the group</p> <p>Low cost</p>	<p>No flexibility</p> <p>Additional legal basis (e.g., consent) may be required in some EU Member States</p> <p>May also come under scrutiny of the DPAs in the near future</p> <p>Acceptance/confirmation/approval procedure in limited EU Member States</p> <p>Do not address circumstances where the exporting entity is a processor established in the EU</p>
Binding Corporate Rules	<p>Global policy document which can be used for all intra-group data transfers worldwide</p> <p>Flexibility</p> <p>BCRs may relate to intra-group transfers of personal data that is controlled by one or more group entities (Controller BCRs), or to data that is processed by the group on behalf of a third-party controller (Processor BCRs)</p>	<p>Time-consuming process (no short-term solution)</p> <p>High cost</p> <p>No standard template</p> <p>Covers only intra-group transfers</p> <p>May also come under scrutiny of DPAs in the near future</p> <p>Burdensome formal acceptance procedure in those EU Member States that recognize BCRs</p>

Legal basis	Pros	Cons
Consent	<p>Quick and efficient</p> <p>Low cost</p>	<p>Can be withdrawn at all times</p> <p>Contested in e.g., employment context (and likely not to be a legal basis in that context under the new EU DP Regulation)</p> <p>Difficult in situations where your organization has no direct contact with the data subject</p> <p>Current requirement of 'unambiguous' consent (which already is not sufficient in some Member States) is likely to change to 'explicit' consent under new EU DP Regulation</p> <p>Strict requirements for obtaining consent in some EU Member States</p> <p>In other EU Member States consent not considered valid for systematic or large-scale transfers</p>
Performance of a contract	<p>Quick and efficient</p> <p>No formalities required</p> <p>Low (no) cost</p>	<p>Not suitable for continual, systematic data transfers in the view of most DPAs</p> <p>Contract must be concluded between the controller and the data subject, or between the controller and third party in the interest of the data subject</p>



Other legal bases include 'necessity of the transfer to protect the vital interests of the data subject', 'for the establishment, exercise or defense of legal claims', and 'necessity or legal requirement of the transfer on important public interest grounds'. These legal bases are only relevant to a limited number of organizations, or in very specific circumstances.

- ☑ Check your (customer) agreements to verify whether any Safe Harbor language is included to legitimize (intra-group) data transfers from the EU to your US affiliate(s). Amend such wording accordingly to reflect the new legal basis (e.g., EC Model Clauses, consent, etc.).

STEP 3. Patch your transatlantic data transfers to third party vendors in the US

If your US vendor and/or its US subcontractor rely on Safe Harbor certification to import data from the EU, contact your US vendor.

- ☑ Verify whether the vendor relies on another legal basis to import EU personal data (e.g., EC Model Clauses concluded with your organization), in addition to its Safe Harbor certification.
- ☑ If not, the US vendor and/or its US subcontractors may enter into controller-to-controller or controller-to-processor EC Model Clauses with the EU data exporting company/ies.
- ☑ If your organization in the EU exporting personal data to a US vendor acts as a data processor: 'Processor-to-(sub-) processor' EC Model Clauses have

not formally been approved yet by the European Commission, so an 'ad hoc' agreement is necessary.

- ☑ Investigate the possibilities of the vendor providing the services from within the EU (e.g., by using EU based servers or systems) and/or choose a subcontractor providing services from within the EU.
- ↳ *Large (US) vendors are already proactively reaching out to their customers to suggest the use of EC Model Clauses, e.g., by sending the template EC Model Clauses which can be added as an addendum to the existing service agreement.*
- ☑ Check the contracts you have in place with your customers in view of warranties made regarding transfers of personal data.

If you warrant that you only transfer personal data (or the personal data of the customers' customers) provided adequate safeguards are in place in the data importing country, you may be in breach of your contract as long as your US vendor and/or its US subcontractors continue to rely on its Safe Harbor certification, or does not offer an alternative.

If your US vendor and/or its US subcontractors do not rely on Safe Harbor and there is another legal basis in place to legitimize the transfer to the US vendor (EC Model Clauses, consent, etc.)

- ☑ Short term: No immediate reaction required.

- ☑ Medium-term: Consider exercising audit rights and verifying sub-processor contracts, as stipulated in the EC Model Clauses.

STEP 4. Review previous notifications to and authorisations from DPAs

Where you have previously notified or registered your (EU) data processing operations with the relevant DPA, such notification or registration may require to be updated in view of any changed legal basis for a transatlantic data transfer (where applicable).

- ☑ Verify whether updates to your existing notifications and registrations, or approvals, are required.

In some EU Member States your data processing operations may be subject to prior authorization of the DPA.

- ☑ Where you have previously obtained such authorization, verify whether an update is required.
- ☑ In cases where you change your data flow set-up, verify whether any additional authorization must be obtained.



HOW CAN WE HELP YOU?

DLA Piper has a dedicated Global Data Protection, Privacy & Security practice consisting of over 150 privacy lawyers across over 30 jurisdictions. Our team has the knowledge and hands-on approach you need in situations such as these, where quick action is required. Please contact us at dataprivacy@dlapiper.com, or liaise with your local DLA Piper contact, to learn more about how we can assist you with developing a compliant approach for your transatlantic data transfers going forward.

DLA Piper is a global law firm with lawyers in the Americas, Asia Pacific, Europe and the Middle East, positioning us to help companies with their legal needs around the world. To learn more, visit www.dlapiper.com.

www.dlapiper.com