OLIVIA WHITCROFT

"Even those who created the rules were finding it difficult to comply with them"

If your company transfers any data to the US, or other countries, then you need to stay on top of the legal rules – or risk huge fines

Woah! It's been over a year since I last updated you on international data transfers.

Those were the days when compliant transfers of personal data to the US seemed impossible. In 2020, the EU-US Privacy Shield was declared invalid, and there began the requirement to undertake transfer risk assessments (TRAs) when using contractual solutions to send data to the US (and other countries). It got worse from there, as it seemed supervisory authorities were not taking a laissez-faire approach to enforcement of the new requirements; for example, the Austrian and French authorities' action against websites using Google Analytics, as covered in my article in issue 343 of *PC Pro*.

In 2023, Meta Ireland was fined €1.2 billion by the Irish Data Protection Commission – the largest GDPR fine ever – for unlawful transfers of personal data to the US. Despite Meta putting extensive supplementary data protection measures in place to address the risks, these were found to be insufficient.

Organisations couldn't escape the risks by relying on well-known platforms. In March 2024, the European Data Protection Supervisor found that the European Commission's use of Microsoft 365 since 2021 infringed data protection law due to a failure to implement appropriate safeguards for transfers outside the EU (including to the US). And the EU Commission wrote the GDPR. So it seems even those who created the rules were finding it difficult to comply with them.

Would transfers to the US ever be lawful again?

Olivia is principal of the law firm OBEP, which specialises in technology contracts, IP and data protection
@ObepOlivia

"The new framework could be an even shorter-lived solution than its predecessor"

Yes, they would...

In 2022, the EU Commission and the US government discussed a new EU-US data privacy framework, and the US President signed an executive order to introduce protections into US law regarding surveillance activities. As from July 2023, EU organisations have been able to transfer personal data to US organisations signed up to the now-approved framework, without the need for other transfer safeguards.

This was followed by a UK extension to the framework (known as the UK-US Data Bridge). Since 12 October 2023, UK organisations can make transfers to US organisations signed up to the Data Bridge, again without additional transfer safeguards.

You can check whether US organisations are self-certified with these regimes at **tinyurl.com/359usdpf**.

Even better, transfers made on this basis don't require exporters to do a TRA, as the EU Commission and UK government have already assessed the risks as part of deciding that the framework is adequate.

...but maybe not for long

Alas, it's not all good news for exporters. Max Schrems is the pioneer of striking out previous EU-US data transfer mechanisms, and the chairman of noyb (**noyb.eu**), a privacy rights organisation. I was fortunate to hear him speak at a conference in September 2023. He took us through some apparent flaws with the new framework and US legal measures. Concerns include that the meaning of the word "proportionate" (for US government surveillance) is not aligned with the EU concept of proportionality, and problems with the new redress mechanism for individuals. It's no secret that noyb has plans to challenge the framework.

He's not the only one spotting problems. In September 2023, the UK ICO published a statutory Opinion, identifying four areas of the UK-US Data Bridge that could pose risks to UK data subjects. First, the definition of "sensitive information" (and therefore the protections applied to such information) doesn't cover biometric, genetic, sexual orientation or criminal offence data. Where included in the transfer, UK exporters should actively specify this additional data as sensitive. It is also unclear how spent criminal convictions are protected, and certain rights for individuals – to withdraw consent, to erasure of data, and to obtain human review of automated decisions – are missing. If relevant in context, UK exporters may want to build in additional protective measures in these areas.

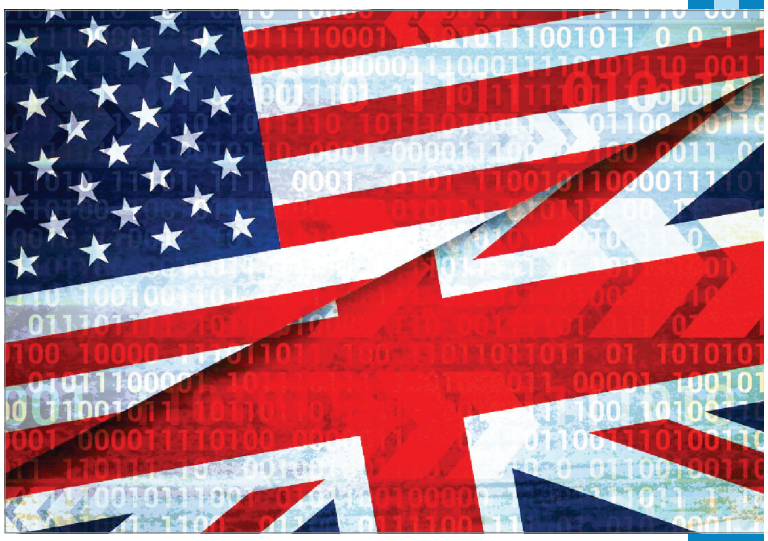
In the same month, Philippe Latombe (a French MP, though acting as a private citizen) applied to the Court of Justice of the European Union (CJEU) for annulment of the adequacy decision for the EU-US framework. His challenge is on several grounds, including inadequacy of privacy guarantees for bulk collection of data, lack of effective remedies for individuals, no framework for automated decision-making, and only vague security safeguards. An application for interim relief (to suspend the adequacy decision) was refused by the CJEU in October 2023, but the main case appears to be ongoing at time of writing.

So the new framework could be an even shorter-lived solution than its predecessor, the Privacy Shield (which lasted four years).

TRA options

Back in March 2023, I was talking about the ICO's new TRA tool. When using this tool, organisations need to carry out an investigation into the laws and practices of the recipient country, unless the data being transferred is all low risk in nature. Although arguably easier to navigate than the EU approach to TRAs (which

BELOW Meta Ireland was hit by the largest ever GDPR fine for unlawful transfers



was the only other ICO-approved option at the time), organisations still reacted with incredulity at the complex task expected of them.

In December 2023, the ICO introduced a new "Option 3" for TRAs, as an alternative to using the ICO tool or EU guidance. It's currently relevant only for transfers to the US, though this is a good country to be relevant for, given the popularity of US transfers.

Option 3 may be used when a TRA is needed because the US recipient is *not* signed up to the UK-US Data Bridge. However, it relies on the UK government's analysis of US laws (in particular, surveillance laws) when assessing the Data Bridge. If you're entering into the UK international data transfer agreement (IDTA) with a US recipient (or putting in place other approved safeguards), you can rely on this analysis for your TRA, without needing to conduct your own review of US laws, as may otherwise be required under the ICO tool. I was disappointed not to hear whoops of joy at this news at a recent training session I gave. But perhaps it's because I'd put all the delegates on mute.

Looking forward, the ongoing validity of Option 3 could go hand in hand with the validity of the Data Bridge. If US legal protections central to the adequacy of the Data Bridge are found to be inadequate after all, surely these could lead to unaddressed risks within the TRA?

Responsibility for TRAs

I had an interesting discussion about how restructuring a supply chain can change responsibility for TRAs. In accordance with UK guidance, the party that is "initiating and agreeing" the transfer must comply with the transfer rules. Let's say delivery of a service involves two providers; one in the UK and one in the US. If you appoint both providers separately, and then send (or instruct your UK provider to send) data to the US provider, you are responsible for the transfer. On the other hand, if you appoint the UK provider to provide the full service, and it partially sub-contracts to the US provider, then the UK provider is responsible for the transfer of data to the US provider for this purpose.

But just because you aren't then responsible for transfer rules and TRAs doesn't mean that the risks of the transfer don't exist, nor that you should simply ignore them. All organisations need to understand their data flows and carry out appropriate checks on providers. This includes checking a provider has carried out an appropriate TRA where needed. Nevertheless, it may still be appealing that the provider is investigating the laws of the country of transfer, rather than you!

Derogations

There are a number of exceptions (or derogations) to the rules on international data transfers. I was brainstorming with my client whether or not a derogation could be used for sending its customer data to a technology provider in the US.

One possible derogation is where the transfer is necessary for performance of a contract between the customer and the controller (in this case, my client). The ICO's interpretation of a transfer being "necessary" is where it is objectively necessary and proportionate for the stated purpose (in this case to perform the contract), and not just necessary as part of your chosen methods.

It's often difficult to argue that it's necessary to transfer data to an overseas provider, where the core purpose of the contract could still be performed without the transfer. For example, if you sell products to UK consumers, it's unlikely to be necessary for you to transfer customer data to an overseas data storage provider. You may need to collect and store customer details in order to fulfil orders, but you *could* use a UK provider or store them in-house. Appointing the overseas provider is simply how you've chosen to run your business.

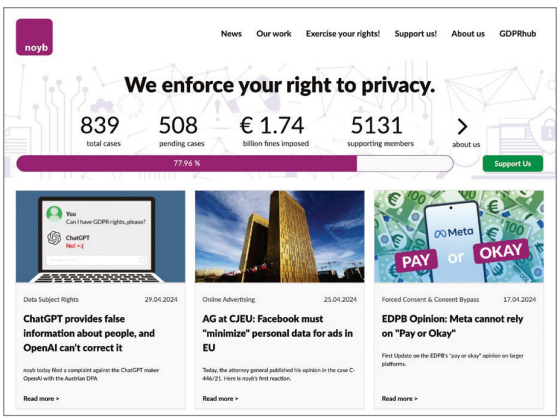
In contrast, UK providers didn't offer functions equivalent to those from my client's US provider (which were core to the customer contract), and my client couldn't provide these functions in-house. So, arguably, the transfer was more likely to be "necessary" for the contract.

However, another matter to assess is whether, rather than relying on the exception, it is more proportionate to put in place a safeguard, such as the IDTA. This is likely to be the case for regular, rather than one-off, data transfer arrangements. As regular transfers were proposed here, the IDTA was probably a better approach.

Use of the IDTA triggers the need for a TRA, which may result in residual significant risks being identified for the transfer of particular data to the US (particularly as this pre-dated Option 3 described above). The ICO's TRA tool then suggests looking at whether exceptions apply in relation to significant risk data. So we can go back to considering the contractual necessity derogation. As the IDTA already provides some protection, it's now more proportionate to rely on this exception for regular (and not just one-off) transfers. The same exception we had rejected therefore becomes a more realistic option to complete the TRA and proceed with the transfer.

ABOVE Data transfers to the US from the UK are still fraught with potential dangers

"It would be sensible for anyone transferring data to the US to think ahead"



BELOW The privacy rights group noyb plans to challenge the new EU-US framework

The saga continues

We're on holiday at the moment, enjoying our hassle-free transfers to the US on the basis of the EU-US framework, UK-US Data Bridge or UK Option 3 for TRAs. But it would be sensible for anyone transferring data to the US to think ahead to what they may do (potentially in a hurry), if the framework is once more struck out. Return data to the UK (or EU)? Restructure your supply chain? Anonymise or reduce the amount of data? Lean more on derogations? Develop your own expertise in assessing risks of US surveillance practices? Or perhaps try to surpass Meta in securing the highest GDPR fine for unlawful transfers?

olivia.whitcroft@obep.uk