OLIVIA WHITCROFT

"I find myself incapable of moving away from my laptop as I await further updates"

Our new regular columnist reveals a tool that can be used to assess the risks of making transfers of personal data to a country outside the UK

It happened again. I was due to run a training course on international data transfers at the end of November 2022. I had prepared a pack of materials, and took great pride in my new case study, taking delegates through the process for a transfer risk assessment. Feeling smug at having completed my work well before the deadline, I sent it all off to the training provider for printing (yes, they like printing stuff).

The following week the ICO decided it was the right time to publish its updated guidance on international data transfers, including a brand-new transfer risk assessment (TRA) tool. So I had to rip up my case study and prepare a new one in a panic. Thanks a lot, ICO.

Avid readers of *PC Pro* will know this is not the first time international data transfer developments have refused to take a break while I write about them (*see issue 333*).

It didn't stop there. The day I ran the course, I shared an interesting nugget of information that the EU had determined that the Republic of Korea has adequate data protection laws, but the UK hadn't followed suit. As soon as the session ended, I spotted an alert that the UK government had, in fact, a few days earlier, decided the Republic of Korea was adequate. Thanks a lot, UK government.

So I find myself nervously sitting here, incapable of moving away from my laptop as I await further updates on data transfers. While I'm here, let me tell you about the ICO's TRA tool.

What is it?

The new TRA tool can be used by companies to assess the risks of making transfers of personal data to a country outside the UK. "Why can't I just use the ICO's International Data Transfer Agreement (IDTA)?" was the first question posed in my training. Well, the *Schrems II* judgment of the EU Court of Justice in 2020 decided that standard contracts (and other approved transfer mechanisms) in themselves may not be sufficient to address every risk, so you need to perform a TRA as well.

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

The ICO's tool helps you to do this, as an alternative to the EU approach. It focuses on six top-level questions, with guidance and decision points during the process. The aim is to determine whether making the transfer would increase the risks to people's privacy and other rights, compared with the risks that exist anyway if the data remains in the UK. There are two key risk headings: risks of a human rights breach, and risks that your transfer mechanism (such as the IDTA) won't be enforceable. Sounds fun, doesn't it?

"There are two key risk headings, including the risk of a human rights breach"

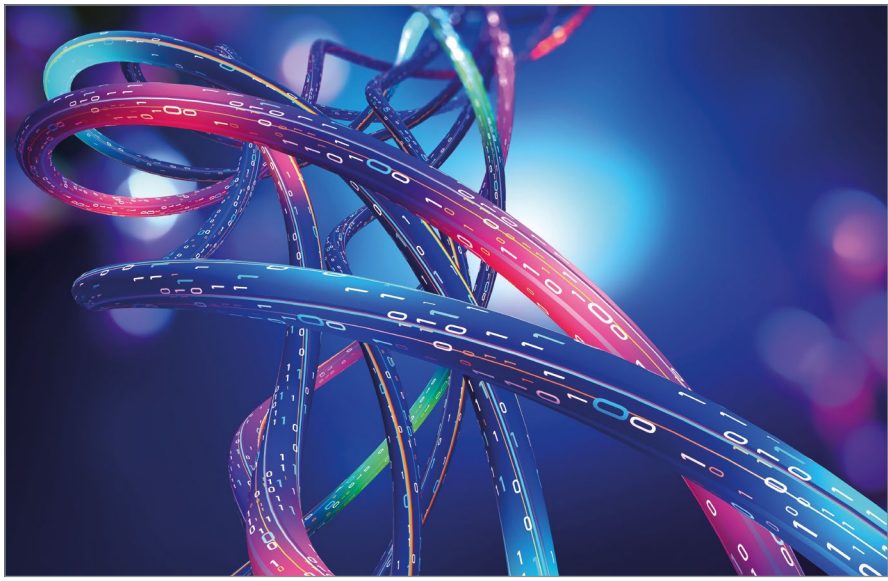
Overview of the tool

The first step is to map out your data flows and, importantly, identify the data you're transferring (question 1). Each category of data is then assigned a "risk score" (question 2). As examples, name and contact details are low risk data, and medical details are high risk data. The risk score may be adjusted up or down with aggravating or mitigating circumstances of the transfer. All going well so far; nothing too tricky to complete.

Then you're told to investigate the human rights risks in the country of transfer (questions 3 and 4). Ah.

This part of the tool spans ten pages, and it's a bit fiendish to get one's head around at first. But it does have a logical structure with questions and decision points. It therefore seems best to communicate it to *PC Pro* readers by means of computer code. I wanted to use the Basic I learnt as a ten-year-old, but my husband has kicked me into the 21st century and helped me write it in Python. So here is a summary of how to determine the level of investigation needed:

```
data_risk = input("What is the risk score for the data
you are transferring?")
 if data_risk == "low":
  level = 0
 else:
  size = input("Are you a small or a big company?")
  if data_risk == "moderate" and size == "small":
   level = 1
  elif data_risk == "moderate" and size == "big":
   level = 2
  elif data_risk == "high" and size == "big":
   level = 3
  elif data_risk == "high" and size == "small":
   volume = input("Are you transferring a little
   amount of data or a lot of data?")
   if volume == "a little":
    level = 2
   elif volume == "a lot":
    level = 3
 if level == 0:
  print("Congratulations, you don't need to
  investigate, and you may transfer the data!")
```



RIGHT Your first step might be to map out your data flows

```
elif level == 1:
  print("You need to do a Level 1 Investigation, but
  don't worry, this won't be too onerous.")
elif level == 2:
  print("You need to do a Level 2 Investigation. A
  little more research to do.")
elif level == 3:
  print("Bad luck, you need to do a Level 3
    Investigation. I'd get some professional advice if I
    were you. Or you may want to see if you can use
    an exception instead.")
```

Now the tool provides some links and guidance to conduct your investigations and decide whether you have concerns that the transfer will significantly increase the human rights risks to individuals. Then, as we march on to question 5, you need to consider enforceability risks in a similar manner. During this process, you can also consider ways to mitigate these risks, using "extra steps and protections" such as technological measures and organisational procedures.

Overall, not so easy! Even the ICO has said "this assessment is undoubtedly complex in many situations". Thanks a lot, ICO.

If, at end of your assessment, you still have what is referred to as "significant risk data", you can consider exceptions to the rules under question 6 – more on this below. If you can't apply an exception, then don't transfer the data.

The position with the US

Another question raised in my course was this: how does this tool work specifically for transfers to the US? Indeed, a lot of data travels to the US, and the whole *Schrems II* case was, after all, specifically about this. Facebook Ireland was transferring data to Facebook US using then-valid transfer mechanisms under the GDPR. But the court decided that US surveillance laws (under the Foreign Intelligence Surveillance Act of 1978) created a risk for data subjects notwithstanding these transfer mechanisms.

There is some disagreement as to the actual risks of US transfers in practice. In a White Paper published in September 2020, the US Department of Commerce indicated that most US companies don't deal in data that is of any interest to US intelligence agencies. This suggests that most transfers wouldn't lead to a significant surveillance risk. But recent decisions of EU supervisory authorities would suggest otherwise. In 2022, the Austrian and French data protection supervisory authorities each issued a decision relating to the use of Google Analytics by website operators. They determined that the websites' use of Google Analytics involved a transfer of personal data to the US. Although measures had been put in place in addition to standard contractual clauses, these weren't sufficient, as they didn't remove the risks of US authorities accessing the personal data. On the other hand, following the Austrian decision, Google issued a statement that it remained convinced that the extensive supplementary measures it offered ensured practical and effective protection of data to a reasonable standard.

The US and the EU have been making progress since *Schrems II* in agreeing a new transatlantic data privacy framework and, at the time of writing, the EU Commission has published a draft adequacy decision for this. On the face of it, this doesn't help with transfers to the US from the UK. But in practice, it may provide more clarity for a UK TRA. If a US company complies with the new EU-US framework, could this reduce the risks to an acceptable level for a transfer from the UK to proceed?

ABOVE US intelligence agencies may be able to access personal data

Use of exceptions

Another great question asked during my training session was whether you can jump to using an exception to the transfer rules, rather than needing to carry out a TRA first. These exceptions (also known as derogations) include obtaining informed consent from the individual or demonstrating that it is necessary to transfer the data for performing a contract with the individual, or for other specified reasons.

Traditionally, the view has been that exceptions could only be used if it were not possible to use another transfer tool, such as the IDTA. This could imply you need to invest time in trying to negotiate the IDTA and carrying out a TRA before reaching a roadblock and moving on to consider exceptions. Although use of the IDTA remains preferable (as it provides more protection for individuals' rights), the ICO's new guidance on applying exceptions refers to first considering if it is more "reasonable and proportionate" to put in place the IDTA (or other transfer mechanism). For the consent derogation, it doesn't even refer to this step.

"There is some disagreement as to the actual risks of US transfers in practice"

Now, use of derogations is not without its own challenges. It may be difficult for consents to be sufficiently informed, and other exceptions require an assessment of the risks to determine "necessity". But the guidance does imply that you can jump to this separate assessment without necessarily having gone through the TRA first, provided you can demonstrate that it is reasonable to do so in context.

Let's get going!

We can now get going with the new-style TRAs and see where they take us. In comparison to the EU approach, in my view the ICO's tool provides clearer steps through the process, with the hope of finding a manageable solution; for example, in relation to low risk data and use of exceptions. Though the difficulties in investigating human rights and enforceability risks remain for many transfer situations.

And don't forget that if the recipient of personal data is in the Republic of Korea, you don't need to do a TRA at all! Actually, perhaps you should do a quick Google search first to check nothing has changed?

olivia.whitcroft@obep.uk

BELOW Facebook has faced problems over data transfers from the EU to the US