EU-US Privacy Shield, Schrems II and transferring data outside the EU – what schools need to know and do

Until 31st December 2020, the UK and EU share the same data transfer protocols. After that, it becomes a different story, which we'll share in a future document.

First, let's look at the EU-US Privacy Shield and how this may affect schools.

What is the EU-US Privacy Shield?

Schools use various products which transfer data to the United States. The UK and the EU have extremely high standards of data protection which are very different to those in the US.

In 2016 it was decided that if US companies met the standards set out in the EU-US Privacy Shield there was adequate protection to allow data to be transferred. The Department of Commerce in the US oversee certification and monitor and enforce these obligations.

So far so good!

Until… the Schrems II case judgment

Then it all changed! On Thursday 16 July 2020, the Schrems II case judgment by the Court of Justice of the European Union (CJEU) found that the EU-US Privacy Shield is no longer a valid way to protect the transfer personal data outside the EEA.

The EU insists that standards of data protection must travel with the data when it goes overseas. If it does not, you may be breaking the law. The concerns, particularly in the US, is that the EU-US Privacy Shield agreement does not prevent the US Government accessing the data when Companies are directly controlled by US laws.

This is not acceptable under EU law.

Can using Standard Contractual Clauses (SCCs) suffice?

Schools, and suppliers in the US, could use SCCs, which is a direct agreement between the supplier and the school and, thus, eliminates US Government involvement. However, the US company has to obey US laws – this opens-up the opportunity for the US Government to access the data the company processes. Therefore, rather than a solution, SCCs could actually be a problem.

The European Data Protection Board has issued advice that urges caution if a SCC is used and highlights the illegality of data transferred without protection and safeguards. It does state that it may be acceptable if the full risks are explained to the data subject and there is an appropriate Lawful Basis to transfer data. Some US suppliers will say that this can be done via Consent, due to how some US laws are worded in schools. However, it would not be appropriate to get every parent, student or staff member to consent before using certain products, you cannot 'force' consent, and so you need to make sure you have an appropriate Lawful Basis.

The good news is that in the UK, the Information Commissioners Office (ICO) has taken a more pragmatic approach saying "We are therefore taking the time to consider carefully what this means in practice. We will continue to apply a risk-based and proportionate approach in accordance with our Regulatory Action Policy."

What GDPRiS schools should do now

- Go to the reports section and run the Brexit Data Location and High-Risk Processing reports these will show you which of your suppliers process personal data in the US
- Go to their supplier listing and view their compliance information, pay particular attention to their Privacy Policy or Data Processing Agreement
- Assess the risk of using that supplier by using our DPIA tool
- Ensure your Privacy Policy is updated to include a specific statement for products that process data outside of the EU
- Ensure the minimum amount of data necessary is being processed