Satswana objection to EU/US Privacy Shield

Summary

If a US organisation wishes to service European customers, then to comply with GDPR and provide their clients with all the protection that affords, all that they need do is locate a server in Europe. First, if they will not do that, then we doubt their intentions. Second, we do not like their "self-certification" and do not consider that their customers should have to conduct further due diligence to ensure the truth of any statement, including whether they have actually signed up for the legal requirements of Privacy Shield, or are just saying they have (Fake Compliance – see Appendix D of our guide). Finally we are concerned that any arising issues would have to be resolved in US Courts, with all the costs and concerns that arise from that.

The "argument" in detail

We should provide some background as a starter. GDPR generally has been accepted worldwide as a personal data privacy standard, regardless of the legal jurisdiction, in the same way as ISO 270001 (for example) has an International following. It is mirrored by DPA 2018 (with a very few changes) so is also entered into English Law, thus after 'Brexit' it will remain the law here. In any event, if you have data held on a Continental child in your School, then you will remain subject to GDPR (for that child's data).

The exception to this universal adoption is the United States, which is gated by its First Amendment, broadly providing freedom of speech. As with the Second Amendment (the right to bear arms) this is fiercely protected in the US. An earlier attempt to maintain data privacy was the Safe Harbour Act, which was declared invalid by the European Court of Justice. Privacy Shield was a replacement for Safe Harbour.

Another bit of background, GDPR has a Regulator as part of the Regulation in every European State, and DPA 2018 has the Information Commissioners Office that will enforce the same law.

Finally, there is the unsatisfactory current status of Processor Contracts, something that the Regulation makes mandatory for any Controller to have in place. For the fullest possible detail on this, please see Appendices D, E and F in our guide that can be found under Resources at www.satswana.com. Put simply there are very few examples of acceptable Processor contracts, with https://tapestry.info/ being a notable and creditable exception. What Tapestry proves is that it can be done, whereas others are either invalid, fake, hopelessly long legal tracts, or non-existent. Even within the UK it is going to take years to arrive at a truly compliant landscape as far as Processor Contracts are concerned.

Let us come to the reasons for our objection to the casual use of the expression "EU/US Privacy Shield" in allegedly GDPR compliant processor contracts.

1. Sorry, some more context first. Privacy Shield is an agreement between the EU and US allowing for the transfer of personal data from the EU to US. The GDPR has

specific requirements regarding the transfer of data out of the EU. One of these requirements is that the transfer must only happen to countries deemed as having adequate data protection laws. *In general the EU does not list the US as one of the countries that meets this requirement.* (Our italics for emphasis.) So the US is NOT regarded as a safe place for data by the EU. But see 2 below.

2 Again more detail, "To join either Privacy Shield Framework, a U.S.-based company *will be required to self-certify* to the Department of Commerce and publicly commit to comply with the Privacy Shield Principles, including the Supplemental Principles requirements. While joining Privacy Shield is voluntary, once an eligible company makes the public commitment to comply with the requirements, the commitment will become enforceable under U.S. law." (Again our italics.) Satswana does not believe that "self-certification" can be relied upon – especially as Class Dojo (for example) claims GDPR compliance by this route, and yet was exposed by The Times as being a company that shared its data with 23 other organisations.

3 Let us consider the phrase "enforceable under US Law". Really? What School has the resources to challenge a provider in the US under their law? Where do you think the sympathy of an American Judge will lie? Why even contemplate the risk when all an ethical provider has to do is to locate their server in Europe to service their European clients? And consider that in Europe you have a Regulator in each Country to fight your battles. Why would anybody want to take on US law in isolation? Why support a provider who does not provide a European Server? Ask yourself why they would not, and you possibly arrive at an answer which would give you cause for doubt.

4 We believe that it is likely that Privacy Shield will go the same way as Safe Harbour, it only takes one legal challenge, either in the US or Europe.

To summarise, on behalf of our customers we do not see why they should take what we see as being an unacceptable risk, against a background of almost impossible absolute due diligence, in using a US based Data Centre. All it requires is that a responsible provider makes a facility available that will be covered by European Law, supported by a Regulator. Then both you, and more importantly the personal data you are entrusted with, is covered absolutely by GDPR. The EU/US Privacy Shield does not do that, and we are fighting against those who would obfuscate that fact.

