Securys®

BRIEFING DOCUMENT

Privacy regulation in a multi-lateral world

International data transfers tensions between regulator and business.

There has always been a tension between governmental interests in keeping citizen data close at hand and the stated commitment to enabling the free flow of data across borders. While the economic benefits of free data flows are generally acknowledged – not least in Convention 108, the 1981 international treaty that deals with data protection – the motives for data protectionism are manifold.

There is a genuine concern for the rights of citizens; other regimes, especially those with lax or non-existent data protection laws, may permit personal data to be abused and exploited by the private sector in ways that cause real harm.

More recently the focus has been on those foreign governments themselves, notably the United States. The arrangement that allowed for the free flow of data between Europe and the US, PrivacyShield, was abrogated by the European Court of Justice in July 2020 pursuant to a legal action brought by Max Schrems, an Austrian privacy activist. The grounds for abrogation were the extent of government surveillance conducted by the US – revealed by Edward →

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) was the first legally binding international instrument in the data protection field.

It remains easier for governments to surveil their own citizens if they keep the relevant data close at hand – Russian and China being the most visible.

Privacy Made Practical®

India, as the likely next major economy to enact a general privacy law, has included a number of data localisation requirements in its draft bill.

Snowden – and the lack of transparency and judicial redress available to non-US data subjects.

However, there are also mercantilist motivations at work. Technology and data are big business; requiring that data be kept in a country or a region not only forces inward investment by foreign technology firms that wish to deal with local data, but also acts as a protectionist barrier which in theory aids the development of the local tech sector. The variance in attitude between the EU (specifically France and Germany) and the UK in this regard is striking. The former have made no real secret of their desire to use regulation to, in their eyes, rebalance the market in favour of home-grown firms, while the latter has tended to take a free-market approach. None of this is surprising in the political context.

Finally, of course, it remains easier for governments to surveil their own citizens if they keep the relevant data close at hand.

China and Russia are the most visible in this regard; both require citizen data to remain in-country – although in both cases it may also be exported provided a copy is retained locally. China has recently made such exports considerably more difficult. A notable feature of countries where this is the motivation tends also to be that local data protection laws do not apply to the state – indeed China combines increasingly stringent controls on the use of personal data by private enterprises with a parallel requirement that they provide open access to that data for the state security services.

India, as the likely next major economy to enact a general privacy law, has included a number of data localisation requirements in its draft bill; all four of the motives listed above are doubtless involved with different weighting in India's decision-making.

Ireland finds itself in a difficult position as a consequence. For a variety of well-understood reasons, it has become the destination of choice for large US technology companies seeking a European base. This has not only had a beneficial, if distorting, effect on the local economy but has also thrust the Irish data protection authority, the DPC, into the spotlight. The original legal action that led to the abrogation of PrivacyShield was brought against Facebook in Ireland, and the DPC has been accused of being dilatory and indeed negligent in its enforcement activity.

The Irish data protection authority has now announced that it intends to require Meta (Facebook) to cease transfers of data from the EEA to the US.

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Faced with these pressures and supported by a judgment in the Irish High Court, and with increasing enforcement activity by both French and German regulators – and German courts – against US tech companies, and specifically with reference to transfers from the EEA to the US, the DPC announced that it intended to require Meta (Facebook) to cease transfers of data from the EEA to the US. However, on judgement day, the 7th August 2022, we learned that the DPC decision on Facebook data transfers is delayed as other watchdogs objected. It is widely known that European officials have clashed over the punitive measures proposed.

Not only will EEA businesses lose access to online advertising revenue and to US-based services, but, in principle, even the transfer of employee data to US parent companies would be barred.

If this order is actually enforced the effects will be striking. The decision will affect the entire EEA – both as a consequence of the Article 60 consistency mechanism and because Meta's EEA headquarters are in Ireland; this could mean the loss of access to Facebook, Instagram and WhatsApp for all EEA residents. Other US-based tech companies will probably face similar enforcement action – most notably Google – and may also be forced to withdraw services. The economic consequences for Ireland would be substantial.

Even services headquartered outside the EEA – such as TikTok, presently operating out of London although plans for a Dublin datacentre have repeatedly been announced and then delayed – will be affected due to the extraterritoriality of the GDPR; they too will be prevented from offering services to EEA residents where such services require the transfer of personal data to countries judged not to have sufficient protection against government surveillance. China, of course, is at least as vulnerable as the US in this regard.

There are wider – and yet more economically damaging – consequences depending on the breadth of enforcement of the transfer ban. Not only will EEA businesses lose access to online advertising revenue (the vast majority of which transacts through Google) and to US-based services such as Microsoft 365 and Google Docs, but in principle even the transfer of employee data to US parent companies would be barred, something that would pose an expensive problem for foreign multinationals and potentially drive employment to other countries – the UK, in particular, is not blind to this given the recent moves to enable unilateral endorsement of free data flows.

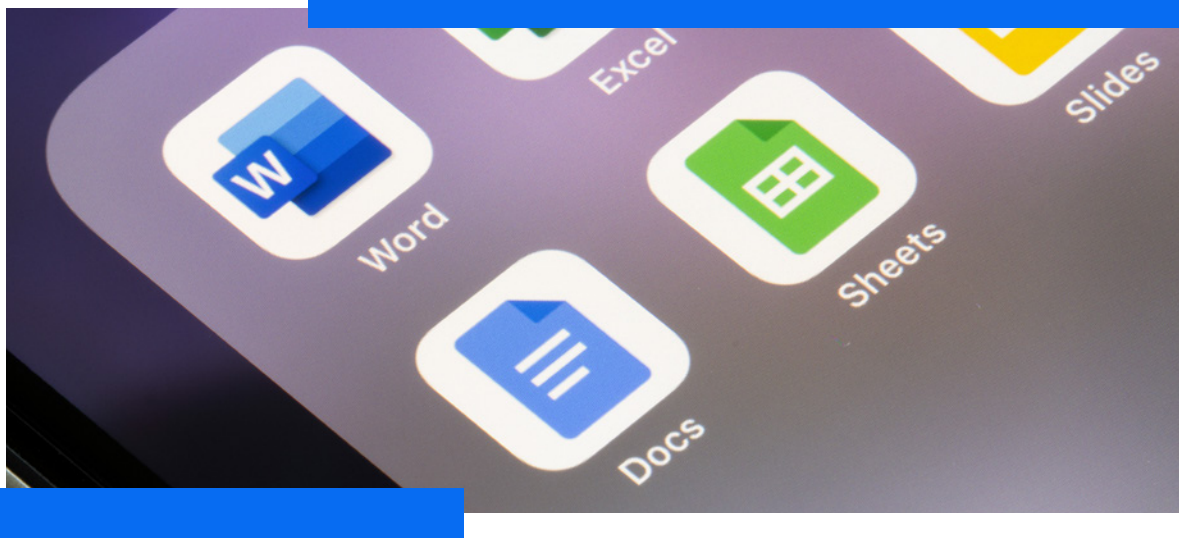
Three options are available to mitigate these risks:

Work is continuing on a replacement for the PrivacyShield arrangement between the EU and the US. Significant progress was announced earlier this year, but at present there is little concrete evidence of a new agreement; the forthcoming November elections in the US may also make it harder for the Biden administration to enact the necessary changes to US surveillance laws.

Services can be completely localised in the EEA. However not only is this expensive for the provider – prohibitively so for all but the largest, it also risks a reduction in service quality since there would then be a strong motivation to focus investment on markets with less restrictive data protection laws. Microsoft has made the most progress in this area – setting up a datacentre in Germany that is operated at arm's length by a German partner. It is important to understand that not only must the data themselves physically be located in the EEA but also all personnel and compute resource with access to that data must be in the EEA. It is the location of processing, not storage, that is relevant in GDPR. The likelihood were this to become the approach is that the quality and variety of services available to EEA residents would be diminished, at least until

EEA = European Economic Area. The EEA aims to strengthen trade and economic relations between each of the 30 EEA countries.

Of any credible EEA-based competitor for Microsoft 365 and Google Docs there is no alternative unless we wish to see a return to on-premises computing or private cloud.



local competition emerged – something it has proven extremely difficult to achieve historically.

More practically, measures are available that allow businesses to legitimise – at least partially – data flows to third countries. These require a formal legal agreement that contains appropriate data protection commitments, including technical and organisational safeguards to minimise the potential for government surveillance. The EU provides a set of standard clauses (SCCs), which must be supplemented by a specific assessment of the risks in each particular case and the associated controls needed to treat the risks. The European Data Protection Board (the collective of EU data protection authorities) has issued guidance on the necessary controls with the caveat that in some cases – such as use of US cloud services – they see no way fully to legitimise the transfer. Some US organisations, notably Microsoft, have committed to the maximum possible lawful resistance to US government surveillance in attempt to address these concerns; an approach that has not yet been tested by either a regulator or a court.

Some US organisations, notably Microsoft, have committed to the maximum possible lawful resistance to US government surveillance.

The present pragmatic approach taken by commercial firms is to localise what they can, introduce the required contractual arrangements and controls and accept the residual risk in transferring what data they cannot – practically or economically – localise. Given the absence, for instance, of any credible EEA-based competitor for Microsoft 365 and Google Docs there is no alternative unless we wish to see a return to on-premises computing or private cloud, either of which would impose unaffordable costs on smaller firms across the EEA. However, any firm taking this line presently faces the risk of enforcement action from EEA data protection authorities including the DPC so long as the underlying prohibition on transfers to the US (and other countries with "excessive" government surveillance) persists.

T 0800 193 8700
E info@securys.co.uk
W www.securys.co.uk
securys-limited

UK0023/0822