To transfer or not to transfer, that is the question

Erik Steiner, Associate and Victoria Hordern, Partner, Taylor Wessing, look at what EU website owners using US service providers can do to ensure that their data transfers are lawful, in the wake of a spate of critical decisions from EU Supervisory Authorities

For many years, the purpose and impact of the rules on international data transfers were relatively peripheral to an organisation's compliance efforts. The cross-border transfer rules under the old Data Protection Directive (95/46EC) were (some might say) more honoured in the breach than in the observance. Although the GDPR's appearance in 2018 didn't fundamentally change this aspect of the framework (elements of Chapter V GDPR reflecting Chapter IV of the Directive), the greater enforcement powers for regulators changed things, plus the mood music had shifted as a result of the Edward Snowden revelations in 2013. The landscape then evolved dramatically in 2020 following the *Schrems II* (C-311/18) decision of the Court of Justice of the EU ('CJEU'). In recent months, we're witnessing the implications of these cumulative developments as European regulators and courts increasingly find data transfers to the US problematic.

Although it seems that complaints about data transfers to the US are being targeted in preference to data transfers to other countries that are less democratic, the focus on the US is primarily because so many of the successful cloud and IT support vendors are US based. In one high profile case, a German publishing company recently found itself subject to a complaint regarding its use of US email marketing platform MailChimp in 2021 for the commonplace activity of using the platform to send out its newsletter. Since the German organisation had not taken the step now required as a result of *Schrems II* and assessed the risk of its subscribers email addresses being sent to Mailchimp — a company subject to the US Foreign Intelligence Surveillance Act ('FISA') — the Bavarian regulator found the data transfers to be unlawful.

Since many and a wide range of entities seem to fall within the reach of the FISA's ambit (witness the Expert Opinion of Professor Stephen Vladeck of November 2021 examining the state of US surveillance laws, www.pdpjournals.com/docs/888224), where does this leave website owners in Europe who use US service providers? With no Privacy Shield replacement immediately in the offing, what can they do to ensure their data transfers to the US are lawful? And what about the vast number of websites that use Google Analytics following the recent critical approach of a number of EU Supervisory Authorities? This article considers some of these cases and suggests some practical measures that organisations can take.

It all started in Austria

The first key decision on data transfers to the US from an EU Supervisory Authority was published in December 2021. The complainant had visited a website on health topics that was formally hosted by an Austrian company while he was logged into his personal Google Account. The website owner deployed the free version of Google Analytics, a tool provided by Google LLC to measure and track website traffic. Data on individuals who visited the website were transferred due to the use of Google Analytics to Google LLC in the US.

The complainant, represented by the NGO None of Your Business ('NOYB'), argued that both the website owner and Google LLC were in violation of the GDPR, since the transfer of his personal data to the US through the tool Google Analytics was unlawful, Google LLC being an 'electronic communications service provider' ('ECSP') under FISA and therefore under an obligation to disclose the personal data of EU citizens on request to the US government.

The procedure before the Austrian Supervisory Authority examining the complaint lasted one and a half years and included multiple submissions in which the respondents (the website owner and Google) pursued two major lines of argument. First, they argued that the transferred data were not personal data under the GDPR. Second, even if the data were considered to be personal data under the GDPR, since the parties had put Standard Contractual Clauses ('SCC') in place plus supplementary measures, the surveillance risk was very low. This was in line with a risk-based approach recognised under the European Data Protection Board's ('EDPB') guidance for transfer tools.

(Continued on page 4)

Victoria Hordern created PDP's eLearning training course, 'International Data Transfers'. For information on the content of this course, see www.pdptraining.com

(Continued from page 3)

In response, the Austrian SA was of the opinion that the transferred data were personal data, since the IP address in connection with other data such as universally unique identifiers was information relating to an identified natural person; a 'data subject'. The SA referred to the CJEU decision in *Breyer* (C-582/14) and implied that even if the person was not logged into his Google Account or no additional data apart from the IP address were transferred, it would still be possible to consider the data as personal data.

Regarding reliance on the SCC for data transfers, the SA referred to the *Schrems II* decision and considered that there is a possibility for a lawful data transfer when combining a SCC with supplementary measures, but these measures need to bridge the existing privacy gap. In this case, while the IP anonymisation feature available for Google Analytics was not implemented correctly, even if it had been implemented, it's probable that this measure would not have been sufficient to bridge the privacy gap given that the anonymisation process only takes place once the data have already been transferred to Google. Further, from the SA's perspective, the measures implemented by Google — for example, the review of access requests from the US government, notifying data subjects of such access requests, and the encryption of data on the server — were not enough to ensure an adequate level of protection under Chapter V of the GDPR.

The Austrian SA's decision, which was given in December 2021, was made against the website owner, since the obligation under Chapter V only applies to the data exporter. However, the SA declared that it would conduct an 'ex officio' investigation and issue a separate decision on the question of whether Google LLC violated its obligations as a processor under the GDPR.

At the time of writing, it is still unclear whether the website owner has filed an appeal against the SA's decision. Since the deadline for an appeal most likely ended at the beginning of February, we should know in the near future.

Other SAs getting in on the act

> ***If it stands, this court decision potentially means that all public and private organisations in Germany cannot use cloud applications offered by US providers where there is a theoretical risk of access to data by US public authorities."***

It has emerged that the Austrian SA's decision on the use of Google Analytics is not a one off. The French Supervisory Authority ('CNIL') issued a statement in February 2022 about a decision it made about the use of Google Analytics. From the statement, it is clear that the CNIL also considers that the measures Google adopted to protect data transferred due to Google Analytics are not sufficient to exclude access by US public authorities. The CNIL ordered a French website to bring its processing through the use of Google Analytics into compliance with the GDPR, or stop using Google Analytics.

Similar concerns about the use of Google Analytics have been expressed by the Dutch and Danish SAs with the Dutch SA putting out guidance indicating that 'the use of Google Analytics may soon not be allowed'. We know that NOYB has instigated a series of complaints to multiple European SAs concerning similar tools and the transfer of personal data. Also, the EDPB has established a task force to coordinate responses to complaints concerning cookie banners filed by NOYB. Therefore, further decisions from European SAs on this issue are expected.

Meanwhile in Germany

There have also been a number of recent decisions from courts in Germany focused on the lawfulness of data transfers to the US.

On 1st December 2021, the VG Wiesbaden (Wiesbaden Administrative Court) issued a provisional court order prohibiting the use of a consent management tool for web cookies known as 'Cookie-Bot'. Cookie-Bot is provided by Danish provider, Cybot and Cybot used a US cloud service provider Akamai Inc. in order to provide its services. Since Akamai is caught by FISA, this made any data transfers to Akamai problematic.

Interestingly, it appears that although Cybot's engagement may have been with an EU subsidiary of Akamai Inc., this arrangement brought the data transfers within the reach of FISA in the eyes of the German court, because the parent company was located in the US. It appears that no SCC or supplementary measures were in place, which is why the court saw a potential privacy risk and prohibited the use of the cookie tool until the end of the proceedings examining the issues on merit. The proceeding on merit is still pending at the time of writing. If it stands, this court decision potentially means that all public and private organisations in Germany cannot use cloud applications offered by US providers where there is a theoretical risk of access to data by US public authorities.

More recently, on 20th January 2022, the LG Munich (Munich regional court) issued a decision on the use of Google Fonts, which focused on the sharing of user IP addresses with Google. Google Fonts allows individuals to choose different fonts for use on their website at no charge — on the face of it, a relatively innocuous service enabling users to explore and implement more creative fonts. In this case, the website owner implemented Google Fonts which when used, required the transfer of the user's dynamic IP address to Google in the US (it seems the website was also not sufficiently transparent with users about the transfer). The IP address was still considered to be personal data even though the user was unidentified.

The court considered the website operator had the legal means to determine identifiability because it retained the dynamic IP address. As personal data, the IP addresses were then transferred to Google in the US and therefore the rules under Chapter V GDPR applied. Whilst the court did not examine compliance with Chapter V in detail, it referred to *Schrems II* and indicated that there was no adequate level of protection for data transferred to the US. Consequently, the court ordered the website owner to pay damages of €100 and to cease and desist from disclosing IP addresses to Google through the use of Google Fonts. The court also indicated that the website owner could be fined up to €250,000 for each violation, or up to six months in prison, for each improper use.

These decisions essentially reflect the same approach as expressed by the Austrian SA to data transfers to the US: that such transfers are generally not permitted (regardless of the relatively inconsequential nature of the data transferred), unless additional measures can be taken to ensure protection. However, it is not yet clear what measures a court or a SA would consider as sufficient. It is unsurprising therefore that organisations are still waiting for the final judicial decisions in these cases, as well as clear guidance from the SAs, before going back to the drawing board regarding their international data transfers.

What should European organisations do in the interim?

Despite the presence of arguments that their reasoning is incorrect, the strict view of EU courts and SAs on data transfers to the US is likely to remain — at least until either the replacement for Privacy Shield is implemented or US surveillance law changes, neither of which seem likely to happen quickly (although at least the Privacy Shield replacement process has momentum).

The recent publication of the draft Data Act from the European Commission indicates that non-personal data is likely to fall under the same type of regime as personal data when it comes to cross-border transfers. The specific provisions dealing with data transfers under the proposed Data Act were included due to the concerns raised about non-EEA governments unlawful access to data. In other words, industrial data should not fall into the hands of unscrupulous foreign governments.

However, there have been recent developments which suggest a clearer path on transfers to the US may be emerging. Google has announced that it is phasing out its Universal Analytics tool to be replaced with (the already launched) Google Analytics 4 which does not rely on logging IP addresses and should help with concerns raised by Supervisory Authorities. Moreover, and more significantly, on 25th March 2022, the US and EU announced they had reached agreement in principle on the new mechanism for data transfers from the EU to the US: the Trans-Atlantic Data Privacy Framework. Whilst at the time of writing the full details of the framework are not known, in order for any new transfer mechanism to confidently withstand judicial challenge, it would necessitate fundamental changes to US surveillance law.

So where does that leave European businesses now and how can European organisations operate internationally if these rules on cross-border data transfers are so strictly interpreted and enforced? The arrangements that European organisations have with US companies that are Electronic Communications Service Providers ('ECSP') are under particular scrutiny. Is it even possible to put forward supplementary measures that will satisfy a EU SA whilst still retaining the utility of the service provided by the US ECSP vendor?

Prompted by the commercial reality, many US vendors are likely to provide further reassurances to their EU customers of the protections they will put in place to help exporters bridge the privacy gap. How appropriate and forthcoming these reassurances will be will depend partly on how privacy savvy the US vender is and whether they have a significant EU customer base. However, European organisations can take some steps to mitigate their risk when engaging with these US vensors. These include:

- selecting the most privacy protective features of any tool or service they are using. If possible, organisations should try to anonymise or pseudonymise any personal data before they leave their platform to be sent to the US;
- employing a local strong encryption solution where the encryption key is held in the EU or an adequate country under the control of the exporter or another trusted party; and
- carrying out a transfer impact assessment before engaging US vendors, setting out the additional protections (supplementary measures) that the exporter and importer will implement.

While UK organisations should keep an eye on these EU developments, it seems unlikely that the Information Commissioner's Office or UK courts would take a similar regulatory enforcement stance on the transfer of personal data associated with tools such as Google Analytics. However, every UK organisation should be prepared to provide evidence of the assessment they have carried out when engaging US vendors for products and services that involve personal data transfers.

Erik Steiner and Victoria Hordern
Taylor Wessing
e.steiner@taylorwessing.com
v.hordern@taylorwessing.com