"PRIVACY SHIELD" FOR EUROPEANS' DATA USE IN US DISSOLVES

July 16, 2020

On July 16, 2020, the European Union Court of Justice ruled that the EU-U.S. Privacy Shield, a compliance policy governing the protection of data transferred from the EU to the United States, was invalid. As a result, U.S. businesses can no longer rely on the Privacy Shield framework in connection with their collection, usage, retention and transfer of personally identifying information about EU residents and citizens.

In the same ruling, the Court of Justice also made it clear that where a business or other entity has taken steps to protect the data it collects, uses, retains and transfers (for purposes of this article, "Utilize") and has contractual provisions in a Privacy Policy or other agreement that have to be accepted by a website or app user, detailing why the entity must Utilize such data. The Utilization can still be compliant with the mandates on Data utilization set forth in the European Union's General Data Protection Regulation ("GDPR"). Standard Contractual Clauses, which have been used in creating privacy language by and for U.S. companies, were generally deemed valid by this ruling, although future disputes may limit their scope.

The GDPR is law across the European Union and applies to all businesses that interact with EU countries' residents or citizens. The purpose of the GDPR is to provide individuals "control of their personal information" – a concept that many within the US, and some within the EU, as implausible and unrealistic. Nonetheless, as the EU has indicated that compliance with the principles and goals of the GDPR should reduce a business's financial liability in the event they are found not to be in strict compliance with the GDPR, businesses with customers who are EU citizens or residents should take ensure their Privacy Policy and internal management policies meet the strictures of the EU.

Such a policy and practice ensure that personal data is collected in a manner seen as legal under the GDPR and then prevent misuse and exploitation of that data while respecting the data's owners' rights – namely, the individual identified by said data.

For any business that relied on the Privacy Shield to deem their Utilization of personal data valid under the GDPR, that shield has now dissolved, and a replacement needs to be put into place rapidly. For all others, a prompt review of their policies to ensure that they comply the guidance on "necessary" transfers and retention, as well as Standard Contractual Clauses where viable, is advised.

Part of the ruling invalidating the Privacy Shield turns on the Court of Justice's judgment of overbreadth of FISA, the U.S. Foreign Intelligence Surveillance Act, which allows the federal government to access data from those who are not U.S. citizens, for law enforcement and national security purposes, without closely tailoring the collection of that data to specific topics, individuals or issues. Congress may this autumn consider legislation to circumvent some of the specific issues set forth by the EU ruling. Until then, the concerns set forth since at least 2017 that the U.S.'s National Security Agency can surveil EU residents and citizens, regardless of whether they are suspected of connections to terrorism, will be maintained, as the EU Court now sees unlimited and unchecked surveillance of EU residents and citizens of Justice as violating the rights protected by the GDPR.

As a result of this ruling, individual businesses cannot themselves claim reliance on or compliance with the Privacy Shield and the provisions it set forth, as the Court of Justice said the principal issue with the Privacy

Shield stemmed from the “limitations on the protection of personal data arising from” FISA. The Court said were “not circumscribed in a way” that is “essentially equivalent to those required under EU law,” as U.S. national security requests for data in the had “primacy” over European citizens’ “respect for private and family life, personal data protection and the right to effective judicial protection,” FISA “condoned” what the Court felt was interference EU citizens’ “fundamental” rights when their data was transferred into or moved through the United States.

Even without earthquakes in how personal data is Utilized, as manifested by this ruling, it is generally seen as a good idea to review and, where necessary, update Terms of Use and Privacy Policy language every five to seven months, and review internal policies on data collection and usage, as well as website and app pop-ups; this ruling provides some guidance on what should be updated in this summer of 2020.

Related Practices

Intellectual Property

Related Practice Teams

Dispute Resolution

Related Team Member(s)

Heidi Howard Tandy