Bloomberg Law

MORRISON FOERSTER

The EU's new e-commerce proposal would preserve European governments' ability to put policies in place that protect personal data privacy and acknowledge that protection as a right.

Photographer: Sebastian Gollnow/picture alliance via Getty Images

INSIGHT: Checking OFAC Lists Is Not Processing of Criminal Data

By Miriam Wugmeister and John Smith

May 16, 2019 4:01AM

Morrison & Foerster attorneys say EU companies should be able to use a sanctions list by the Office of Foreign Assets Control to screen for illicit activity that could cause them harm. Some EU companies, however, are afraid to use that list because they believe, inaccurately, that sanctions list screening may constitute the processing of criminal data. This is not correct, and EU companies should continue accessing this type of public information to help them thwart financial system abuses.

One ongoing concern of EU companies is that they may no longer be able to use various economic sanctions lists—such as the Specially Designated Nationals List ("SDN List") put out by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC)—to screen for illicit activity and thereby prevent reputational, legal, and business risks.

Because the General Data Protection Regulation (GDPR) delegates the rules for the processing of "personal data relating to criminal convictions and offences" to member state control, compliance officials remain concerned that banks and other companies may be barred from using publicly available, government-issued lists that provide critical information to help them avoid doing business with terrorist financiers, weapons of mass destruction (WMD) proliferators, money launderers, and other illicit actors.

Their concerns are based on the view that checking OFAC and other sanctions lists might constitute processing of criminal data. However, this characterization is incorrect for a simple reason—people are not placed on these lists because they are accused or convicted of a crime. They are put on the lists because they have violated some civil norm.

Getting on the List

To be added to the OFAC list, SDNs need not be convicted of any crime; in most cases, no criminal charges are ever even sought by prosecutors in the United States or other jurisdictions.

Instead, as OFAC notes on its website, "SDNs are individuals and entities located throughout the world that are blocked pursuant to the various sanctions programs administered by OFAC. SDNs can be front companies, parastatal entities, or individuals determined to be owned or controlled by, or acting for or on behalf of, targeted countries or groups."

It is true that some of the actions for which an individual or entity may be added to a U.S., EU, or U.N. sanctions list—such as support for terrorism and WMD proliferation—can also serve as the basis for separate criminal charges. The purposes underlying U.S., EU, and United Nations sanctions, however, are preventative, not punitive, as in the criminal context.

Sanctions Lists Meant to Deter Bad Behavior

The sanctions lists are intended to deter continuing bad behavior and prevent abuse of the U.S. and international financial systems, per international obligations such as those contained in the Recommendations of the Financial Action Task Force endorsed by more than 180 countries, as well as the EU's Fourth Anti-Money Laundering Directive, which calls for "the use of evidence-based decision-making in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively."

There is ample reason to utilize separate criminal and administrative actions to target similar behavior.

U.S. and European prosecutors may not want to waste their limited resources bringing criminal charges against every terrorist financier who hides behind the protection of powerful home country officials, or every kleptocrat stealing a developing nation's wealth but whose lack of local ties may not allow another country's criminal authorities to make a case.

Western prosecutors may not want to attempt to jump through the necessary hoops to use classified evidence to indict every Iranian, North Korean, or Russian cyber actor whose manipulative keystrokes wreak havoc on Western public and private sector entities, especially when those actors will never set foot outside their home countries.

And sanctions lists can protect banks and other industries from facilitating, or succumbing to, such abuses of the international financial system, even when the criminal tool is not readily available or practicable.

Benefits Outweigh Burden

The consequences of being added to the OFAC or other sanctions lists fall far short of those that result from a criminal conviction. No jail time is threatened or even possible as a result of an SDN listing, unless U.S. or foreign prosecutors initiate totally separate criminal charges based upon their own criminal cases.

The only legal consequences that flow from listings as SDNs are, first, any property subject to U.S. jurisdiction must be frozen–or "blocked," to use sanctions terminology–and, second, Americans are prohibited from dealing with SDNs. These consequences, while severe, do not rise to any legal or common-sense interpretation of "criminal convictions."

The "freezing" of assets required by an SDN listing also differs substantially from the "seizing" of assets that may result from a criminal conviction. When assets are frozen, title remains with the SDN, interest continues to accrue, and, barring a separate criminal or civil action, the funds are generally returned to the SDNs upon their removal from the list. When assets are seized pursuant to a criminal proceeding, title transfers to the state and they are not returned.

Indeed, the legal standard by which OFAC acts is far less than the "beyond a reasonable doubt" standard for criminal cases and even the "preponderance of the evidence" standard for civil cases. As the U.S. federal courts have repeatedly emphasized, OFAC's SDN listings are held to the lower "reasonable basis" legal standard applicable to federal agency action.

There are ample objectives underpinning the GDPR's restriction on the use of criminal data. Preventing banks and other companies from utilizing publicly available information—unrelated to a criminal offense but compiled to protect the international financial system from abuse—is not one of them.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

Miriam Wugmeister is co-chair of Morrison & Foerster's market-leading Global Privacy and Data Security Group and ranked among the top in the profession by all major legal directories. She is regularly called upon by some of the world's largest and most complex multinational organizations to confront their most difficult U.S. and international privacy challenges. Having helped hundreds of clients respond to data security incidents, Ms. Wugmeister has worked on several of the most noteworthy and largest data security incidents over the past few years.

John E. Smith, former director of the U.S. Treasury Department's Office of Foreign Assets Control, is co-head of Morrison & Foerster's National Security practice. He has unmatched experience in economic sanctions, enforcement, and national security. Both in the U.S. and globally, clients turn to Mr. Smith for his deep experience and unique perspective on the complexities and escalating risk of U.S. and multilateral sanctions.