ICLG

The International Comparative Legal Guide to:

Anti-Money Laundering 2018

1st Edition

A practical cross-border insight into anti-money laundering law

Published by Global Legal Group with contributions from:

Allen & Overy LLP
ANAGNOSTOPOULOS
ASAS LAW
Barnea
BONIFASSI Avocats
C6 an Acuris Company
Castillo Laman Tan Pantaleon & San Jose Law Offices
Chambers of Anuradha Lall
Debevoise & Plimpton
DQ Advocates Limited
Drew & Napier LLC
DSM Avocats à la Cour
Duff & Phelps, LLC
Durrieu Abogados S.C.
EB LEGAL
Encompass
Gibson, Dunn & Crutcher LLP
Hamdan AlShamsi Lawyers & Legal Consultants
Herbert Smith Freehills Germany LLP
JMiles & Co.
Joyce Roysen Advogados
Kellerhals Carrard Zürich KlG
King & Wood Mallesons
Linklaters
Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL.
Navigant Consulting
Rato, Ling, Lei & Cortés – Advogados
Rustam Kurmaev & Partners
Shri Singh
WilmerHale
Yamashita, Tsuge and Nimura Law Office

glg
global legal group

global legal group

Contributing Editors
Joel M. Cohen and Stephanie Brooker, Gibson, Dunn & Crutcher LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Senior Editors
Suzie Levy
Caroline Collingwood

CEO
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
June 2018

ISBN 978-1-912509-12-6
ISSN 2515-4192

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Implications of the E.U. General Data Privacy Regulation for U.S. Anti-Money Laundering and Economic Sanctions Compliance

Sharon Cohen Levin

Franca Harris Gutierrez

WilmerHale

I. Introduction

Many financial institutions will confront a new compliance challenge on May 25, 2018, the effective date of the European Union's revamped data privacy law, the General Data Protection Regulation ("GDPR"). In short, GDPR data use *restrictions* conflict with data use *requirements* imposed through U.S. anti-money laundering ("AML") and economic sanctions laws.

The GDPR imposes stringent limitations on processing E.U. residents' personal data. Under this new regime, institutions will be unable to receive, or produce to U.S. authorities or courts, any personal data about their own E.U. customers or customers of their E.U. affiliates *unless* they can identify a GDPR-recognised "lawful basis" to do so. Compliance with U.S. AML and economic sanctions law may require the use of data subject to these restrictions, including customer-identifying information and transaction data. Even though this data is in many cases needed for U.S. law compliance, U.S. AML and economic sanctions laws do not provide an obvious "lawful basis" to process data subject to the GDPR. Navigating these conflicting regimes may expose a financial institution to significant liability if they violate either U.S. or E.U. law.

This article first provides an overview of U.S. AML and economic sanctions laws and the GDPR. The article then analyses the conflicts between the two legal regimes and possible approaches for institutions to minimise such conflicts.

II. The E.U. General Data Privacy Regulation Framework

The GDPR expands upon and replaces the E.U.'s existing data privacy framework, the E.U. Data Protection Directive ("Directive"), to regulate the "processing" of "personal data".[1] While many GDPR requirements align with the Directive, there are significant new provisions in the GDPR, including increased maximum penalties.

A. Covered Data

Under the GDPR, as under the Directive, "personal data" is defined to include any information that could be used to identify any natural person, for example, a name, an identification number, an online identifier, or even location data.[2] Importantly to U.S. AML and economic sanctions obligations, the GDPR regards personal data relating to criminal convictions and offences as particularly sensitive and thus only allows the processing of such information "under the control of official authority or when the processing is authorized by [E.U.] or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects".[3]

B. Restrictions on Processing

In general, personal data is deemed "processed" and thus subject to the GDPR's restrictions any time it is used, collected, retrieved, stored, transferred, disclosed, restricted, altered, or erased, whether through automated processes or manually.[4] The GDPR imposes separate requirements for the processing of data within the European Economic Area ("E.E.A."),[5] the transferring of data from the E.E.A. to locations outside of E.E.A., and the production of personal data to authorities outside of the E.E.A.

1. Processing Data Within the E.E.A.

There are six lawful bases for processing non-sensitive personal data *within* the E.E.A. Those bases are (a) "freely given, specific, informed and unambiguous" consent;[6] and circumstances where processing is necessary, (b) for the performance of a contract with the individual data subject,[7] (c) for compliance with *E.U. or Member State* law, which may include E.U. AML or sanctions laws,[8] (d) for the protection of the life or health of a person (*i.e.*, "vital interests"),[9] (e) for the public interest,[10] or (f) for overriding legitimate interests.[11] Where any one of these bases is present, the processing of personal data within the E.E.A., and the transfer of that data from one place to another place in the E.E.A., are generally permitted.

2. Processing Personal Data Outside of the E.E.A.

For an institution in the U.S. or otherwise outside of the E.E.A. to obtain personal data about its E.U. customers or customers of its E.U. affiliates, additional requirements must often be met. These additional requirements for transferring personal data outside the E.E.A. pose the greatest difficulties for compliance with U.S. AML and economic sanctions laws.

In addition to identifying a lawful basis, additional requirements apply in the following scenarios: (i) an E.U. institution seeks to transfer personal data to a U.S. parent or affiliate; and (ii) a U.S. institution that is itself subject to GDPR (because it serves E.U. residents and markets or monitors customer behavior in the E.U.) attempts to obtain personal data about E.U. customers from *any source*.[12] In either of these scenarios, there must be a lawful basis for the data to leave the E.E.A. *and* the institution receiving the data must be within a country the European Commission deems to offer an adequate level of data protection[13] or must otherwise demonstrate that it adequately protects data. Institutions in countries not deemed "adequate", such as the U.S., must guarantee that they adequately protect data by entering into internal agreements with E.U. affiliate

companies from whom they intend to receive data that contain Standard Contractual Clauses ("SCC").[14] If no such data protection guarantee exists, transfer is permitted only if one or more specified "derogations" exists, for example, explicit informed consent or the "establishment, exercise, or defence or legal claims".[15]

3. Producing Data to Non-E.E.A Authorities and Courts

The GDPR places new restrictions on the production of covered personal data to courts, tribunals, and administrative authorities outside of the E.E.A. – such as the U.S. Department of Justice ("DOJ") and Treasury's Office of Foreign Asset Control ("OFAC"). Under the GDPR, requests or demands for covered personal data from a non-E.E.A. authority, court, or tribunal are not "recognised or enforceable in any manner" unless they are based on an international agreement, such as a mutual legal assistance treaty ("MLAT"), in force between the requesting country and the E.U. or Member State.[16] This requirement is expressly "without prejudice to other grounds for transfer", however, so productions to DOJ or another U.S. authority may still be allowed if a derogation under the GDPR exists.[17]

C. Penalties

The GDPR provides for a maximum administrative fine of €20,000,000 (roughly $25 million) or 4% of the company's "global turnover" (*i.e.*, global revenue), whichever is greater.[18] Before the GDPR, the maximum fine for a data protection violation in most E.U. Member States was under €1 million; even in France, which allowed for a maximum fine of €3 million, the largest fine ever imposed was less than €1 million. The GDPR also allows Member States to impose criminal penalties for certain violations at the discretion of those Member States.[19]

III. U.S. Anti-Money Laundering and Economic Sanctions Framework

Financial institutions in the U.S. are subject to extensive anti-money laundering and economic sanctions laws and regulations. Non-compliance with these requirements can result in significant civil or even criminal penalties.[20]

A. U.S. AML Requirements

The Bank Secrecy Act ("BSA") as amended by the USA PATRIOT Act of 2001,[21] the BSA's implementing regulations,[22] and guidance issued by U.S. regulators establishes the federal scheme of anti-money laundering laws in the U.S. (collectively, the "AML Rules"). The U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") is charged with implementing key aspects of the federal anti-money laundering scheme.

The AML Rules require banks, broker-dealers, and certain other financial institutions[23] operating in the U.S. to serve as a first line of defence against money laundering and terrorist financing. U.S. financial institutions must implement an effective AML program[24] incorporating multiple elements prescribed by regulation.[25] Two of these elements present particular challenges for customers whose data is subject to the GDPR. First is FinCEN's Customer Due Diligence ("CDD") Rule, which became effective on May 11, 2018. The CDD Rule demands that financial institutions collect extensive personal information about their customers and build comprehensive profiles of those customers' behaviour.[26]

Second, financial institutions must also conduct ongoing monitoring of their customers' behaviour. In addition to updating each customer's profile as needed, institutions must file a Suspicious Activity Report ("SAR") with FinCEN any time the institution "knows, suspects, or has reason to suspect" that a transaction that aggregates to $5,000 or more involves illegally derived funds, is designed to evade BSA requirements, or has "no business or apparent lawful purpose". The information needed to perform effective due diligence, monitor customer behaviour, and file SARs will be subject to GDPR restrictions for E.U. customers.

Violations of AML Rules, such as failure to maintain an effective AML program or failure to file SARs, could result in significant civil monetary penalties, fines, and forfeiture. Where the violation of the AML Rules is "willful", institutions and involved individuals may also face criminal penalties.[27] Participation in a money laundering scheme or the knowing receipt of proceeds from criminal activity is also a crime that can result in additional penalties, including imprisonment for involved personnel.[28]

B. U.S. Economic Sanctions Requirements

U.S. financial institutions must also collect personal data about their customers to ensure the customers are not subject to, owned by parties subject to, or affiliated with countries or regions subject to, U.S. economic sanctions programs administered and enforced by OFAC.

OFAC maintains a list of Specially Designated Nationals and Blocked Persons ("SDN") to whom U.S. persons – which includes institutions *and their foreign branches* – may not provide services.[29] Those institutions and branches must routinely screen customers to determine if any customer or certain beneficial owners are subject to sanctions.

OFAC also maintains country-based sanctions programs prohibiting U.S. persons from trading with specific countries or territories, such as Iran, North Korea, Syria, and Cuba,[30] and similar "sectoral" or "hybrid" sanctions relating to Russia and Venezuela.[31] While most sanctions programs apply to U.S. companies and their foreign branches, the Iran and Cuba sanctions programs also apply to *foreign-incorporated subsidiaries* of U.S. companies, meaning that entities in the E.U. must comply with these sanctions programs if their parent is a U.S. institution.[32]

In practice, both list-based sanctions and country-based sanctions require institutions to use information that may be subject to GDPR data use restrictions.

Failure to comply with U.S. sanctions law can result in significant consequences, as OFAC takes a strict liability approach to enforcement. The fines OFAC impose can be substantial, particularly if the involved institution did not "voluntarily disclose" the violation or did not maintain an adequate compliance program or due diligence processes.[33] Where violations are willful, DOJ can impose significant criminal penalties and fines.[34]

IV. Implications

U.S. AML and economic sanctions laws and the GDPR are rife with conflict, and noncompliance with either presents significant risk. It does not help matters that neither the U.S. nor the E.U. recognise the other's law as a legitimate basis for noncompliance with its own regime. The primary implication for financial institutions is that, unless and until solutions arise after GDPR implementation, the conflict between the GDPR and U.S. AML and economic sanctions laws cannot be completely resolved. There are, however, steps financial institutions can take to mitigate the potential impact of these conflicts.

A. E.U. Authorities' Response to U.S. Obligations

E.U. financial institutions can generally rely on E.U. AML and sanctions laws as a recognised "legal obligation" – *i.e.*, one of the

lawful bases – to collect and use customers' personal data within the E.U.[35] The difficulty arises when those E.U. institutions seek to *transfer* such data to U.S. affiliates, or when U.S. institutions subject to the GDPR independently attempt to collect data about E.U. customers. In either of these circumstances, even assuming a Standard Contractual Clause or other recognised legal instrument exists for the transfer of the data to the U.S., it will be difficult for institutions to identify a "lawful basis" for the transfer that E.U. authorities are sure to accept.

Historically, financial institutions have relied on consent when seeking to process personal data covered by E.U. data privacy laws, but the GDPR makes obtaining valid consent considerably more difficult. Under the GDPR, consent must be a "freely given, specific, informed and unambiguous".[36] The GDPR further specifies that "[i]f the data subject's consent is given in the context of a written declaration which also concerns other matters", the data processing consent request must be "clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language".[37] Further, "[w]hen the processing has multiple purposes, consent should be given for all of them".[38] The GDPR also provides that consent is revocable at any time.[39] Thus, consent is no longer a reliable lawful basis for institutions to collect or transfer large amounts of information about E.U.-resident customers to the U.S. Obtaining consent as a *secondary* basis for the data transfer, however, is often prudent.

The "legal obligation" justification is also precarious. First, the GDPR unequivocally refuses to recognise U.S. law (or any other non-E.U. country law) as a "legal obligation" justifying the processing of E.U. residents' personal data. Thus, E.U. data protection authorities are unlikely to be swayed by an argument that data needed to be transferred to the U.S. to satisfy *U.S.* AML and economic sanctions laws. However, if an institution provides services in the E.U. but conducts its global, enterprise-wide compliance functions out of the U.S., as many multinational financial groups headquartered in the U.S. do, then *E.U.* AML and sanctions laws can arguably provide the "legal obligation" justifying the transfer of data to the U.S. This will be helpful in the AML context, given the substantial overlap between U.S. AML laws and E.U. AML laws; but it will not always help with data transfers to comply with U.S. economic sanctions laws, because OFAC sanctions lists will not always match E.U. and U.N. sanctions lists. Further, it is unclear whether E.U. data protection authorities will accept this invocation of the "legal obligation" lawful basis, given their general scepticism of transfers of data to the U.S.

Absent a clear lawful basis to transfer E.U.-resident customer data to the U.S. under the GDPR, U.S. institutions will have difficulty obtaining the information they need to conduct effective AML programs and to ensure that they and their foreign affiliates do not provide services to individuals and entities subject to OFAC sanctions. U.S. institutions will also have difficulty responding to requests from U.S. prosecutors, regulators, and courts, for documents containing personal data subject to the GDPR, as the GDPR provides that such requests are to be ignored unless procured by MLAT or other international treaty device.

B. U.S. Authorities' Response to E.U. Obligations

In general, U.S. prosecutors and regulators have been sceptical of arguments that U.S. financial institutions could not obtain information needed to effectively conduct AML and economic sanctions monitoring and screening because of E.U. privacy restrictions.[40] Indeed, DOJ and OFAC have pursued U.S. financial institutions even where violations were caused or exacerbated by the fact that the U.S. institution could not obtain customer information from a European affiliate, and DOJ has demanded that U.S. parent companies produce data stored abroad with their subsidiaries in Europe.[41] Institutions that are subject to deferred prosecution agreements have even greater difficulty convincing DOJ to give credence to E.U. data privacy laws; in this scenario, it can appear to the DOJ that the companies are selectively refusing to provide data, and the DOJ will usually insist that the data be produced.

In the past, juxtaposed with DOJ's and OFAC's routine imposition of multi-million-dollar – and in some recent sanctions cases, billion-dollar – penalties, E.U. data protection penalties were often considered trivial. E.U. data protection authorities rarely enforced E.U. data privacy laws and, even when they did, they rarely imposed fines of millions of dollars. U.S.-based financial institutions therefore tended to prioritise compliance with U.S. AML and economic sanctions laws and U.S. authorities' requests for information when they came into tension with E.U. data privacy laws. Relatedly, U.S. financial institutions have typically ultimately acquiesced to DOJ's requests for data stored in the E.U., even if there is arguably a basis to refuse such requests under E.U. data privacy laws. The potential for substantial penalties under the GDPR could alter these dynamics.

C. Steps Forward

The GDPR has and will continue to change the way financial institutions balance their U.S. AML and economic sanctions obligations and their E.U. data privacy obligations, but it is unclear whether it will cause U.S. prosecutors and regulators to revisit their approaches to civil and criminal investigations and penalties. There are some general steps that U.S. financial institutions can take to prepare:

1. *Determine whether your institution is subject to the GDPR.*
   - As a threshold matter, institutions should carefully assess whether any of their U.S. operations are subject to the GDPR by considering whether those operations serve customers living in the E.U. and whether they market in the E.U. or monitor customer behaviour in the E.U.
   - Institutions that conclude that they are not themselves subject to the GDPR should consider to what extent they need to obtain personal information from affiliates in the E.U., for example, affiliates for whom they provide U.S. dollar clearing functions.
2. *Identify a lawful basis for obtaining data from the E.U.*
   - Institutions that conclude that they *are* subject to the GDPR should identify the lawful basis or bases on which they will rely to obtain personal data about E.U. customers.
   - Institutions that conclude that they are not themselves subject to the GDPR, but that need to obtain personal information from affiliates in the E.U., should confirm that the E.U. affiliates have identified a lawful basis to transfer data to the U.S.
3. *Ensure that notice and consent forms are GDPR-compliant.*
   - Because consent may be a lawful basis in certain circumstances, institutions subject to the GDPR or that have E.U. affiliates should ensure that E.U. customers receive customer notice and consent forms that specify that personal data will be transferred to the U.S. to comply with U.S. AML and economic sanctions laws. The forms provided to customers must be unambiguous and not unduly long or complex.
4. *Ensure that adequate data protection safeguards exist.*
   - Institutions should carefully review any existing standard contractual clauses or other data protection agreements

with E.U. affiliates from whom they receive personal data to ensure that the agreements cover all data processing activities in which the institution engages for AML and economic sanctions purposes.

5. *Prepare for prompt notification in the event of a data breach.*
   - Institutions should ensure that they have mechanisms in place to issue data breach notifications to data protection authorities within 72 hours of discovering any such breach and promptly to affected customers.
6. *Appoint a Data Protection Officer.*
   - Institutions subject to the GDPR should appoint a Data Protection Officer to oversee their GDPR implementation and compliance going forward.
7. *Monitor GDPR developments.*
   - The Article 29 Working Party is an advisory body of representatives from each E.U. Member States' data protection authority, the European Data Protection Supervisor, and the European Commission. The Working Party continues to issue guidance concerning the application and interpretation of the GDPR, which should be considered an evolving body of law. Institutions should monitor guidance from the Working Party to ensure that their understanding and implementation of GDPR requirements are up to date.

These recommendations are intended to provide general guidance, but they should not replace more tailored advice focusing on the needs and operations of particular institutions.

V. Conclusion

The GDPR generates new questions and concerns for U.S. financial institutions that directly provide services to E.U. residents or must coordinate their compliance functions with financial institutions in the E.U. Financial institutions' U.S. AML and economic sanctions obligations, which require collection of personal information about customers, is in tension with the GDPR, which generally does not recognise these obligations as a lawful basis to process E.U. residents' data. Although the regulatory environment in both the U.S. and E.U. will evolve upon implementation of the GDPR and much remains unclear, institutions must be aware of these tensions and take certain measures to prepare.

Endnotes

1. Regulation (E.U.) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union ("GDPR"). While E.U. Member States were required to implement the Directive through local implementing statutes (which varied from E.U. Member State to Member State), the GDPR will automatically apply to all E.U. Member States. E.U. Member States will be permitted, however, to enact national legislation to advance specified interests.
2. GDPR Article 4(1).
3. Article 10.
4. *Id.*
5. The E.E.A. includes the countries in the E.U. as well as Iceland, Lichtenstein, and Norway. It remains to be seen whether the U.K. will remain part of the E.E.A. after Brexit.
6. GDPR Article 6(1)(a).
7. GDPR Article 6(1)(b).
8. GDPR Article 6(1)(c).
9. GDPR Article 6(1)(d). *See* Recital 46; Recital 49. This basis would not seem to apply for financial institutions seeking to process personal data in order to ensure AML and economic sanctions compliance.
10. GDPR Article 6(1)(e). *See* Recital 45. The U.K. Information Commissioner's Office ("ICO") guide to the GDPR lists private water companies as an example of an entity that may rely on this lawful basis. *Guide to the General Data Protection Regulation (GDPR)*, ICO, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ ("ICO Guide"). This basis would not seem to apply to financial institutions seeking to process personal data in order to ensure AML and economic sanctions compliance.
11. GDPR Article 6(1)(f).
12. GDPR Article 44; GDPR Article 45; Recitals 78–91.
13. *See* GDPR Article 45; Recital 103.
14. GDPR Article 46.
15. GDPR Article 46. For accepted derogations, *see* GDPR Article 49(1).
16. GDPR Article 48.
17. *See* GDPR Article 48; GDPR Article 49.
18. GDPR Article 83(4)-(5).
19. *See* GDPR Article 84(1).
20. *See* 31 U.S.C. § 5321; 31 U.S.C. § 5322; 31 CFR Appendix A to Part 501; 12 CFR § 12.21; 12 CFR § 21.11; 12 CFR § 163.180.
21. *See* 31 U.S.C. § 5311 *et seq*.
22. *See* 31 C.F.R. Subt. B, Ch. X.
23. 31 U.S.C. § 5312(a)(2) and (c)(1). *See* 31 C.F.R. § 1010.100(t).
24. *See* 31 U.S.C. § 5318(h); 31 C.F.R. § 1010.210. *See also* Fed. Fin. Inst. Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual 28 (2014) ["FFIEC Examination Manual"].
25. *See* Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29420 (May 11, 2016) (codified at 31 C.F.R. § 1010.230) (describing the "five pillars" of an effective AML program) ["CDD Rule"].
26. *See* CDD Rule, 81 Fed. Reg. 29398. A bank must file a Suspicious Activity Report ("SAR") with FinCEN any time the bank "knows, suspects, or has reason to suspect" that a transaction that aggregates to $5,000 or more involves illegally derived funds, is designed to evade BSA requirements, or has "no business or apparent lawful purpose". 31 C.F.R. § 1020.320. Other financial institutions are also subject to specific SAR requirements.
27. 31 U.S.C. § 5321; 31 U.S.C. § 5322;12 U.S.C. § 1818(i); 31 C.F.R. Appendix A to Part 501.
28. 12 U.S.C. § 1956; 12 U.S.C. § 1957.
29. OFAC Specially Designated Nationals and Blocked Persons List, https://www.treasury.gov/ofac/downloads/sdnlist.pdf (last updated Apr. 6, 2018).
30. *See* Sanctions Programs and Country Information, U.S. Dept. of Treasury, https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx (last updated Apr. 6, 2018).
31. *See e.g.*, Executive Order 13662 (Mar. 20, 2014); Executive Order 13808 (Aug. 24, 2017).
32. 31 C.F.R. § 560.215; 31 C.F.R. § 515.329. *See also* OFAC FAQ, U.S. Dept. of Treasury, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx.

33. *See, e.g.*, *Settlement Agreement Between U.S. Dep't of the Treasury, Office of Foreign Asset Control, and Crédit Agricole Corporate and Investment Bank*, COMPL 1000368 (Oct. 15, 2015), https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20151020_cacib_settlement.pdf (settling for a $330 million fine for egregious violations not voluntarily disclosed).
34. *See* 50 U.S.C. § 1705. *See also* Press Release, U.S. Dep't of Justice, *ZTE Corporation Agrees to Plead Guilty and Pay Over $430.4 Million for Violating U.S. Sanctions by Sending U.S.-Origin Items to Iran* (Mar. 7, 2017), https://www.justice.gov/opa/pr/zte-corporation-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions-sending (imposing a combined penalty of $1.19 billion with Dep't of Treasury and Dep't of Commerce).
35. Indeed, the U.K. ICO's Guide on the GDPR specifies that a financial institution may "rel[y] on the legal obligation imposed by the Part 7 of Proceeds of Crime Act 2002 [one of the U.K.'s chief anti-money laundering laws] to process personal data in order submit a Suspicious Activity Report to the National Crime Agency when it knows or suspects that a person is engaged in, or attempting, money laundering". ICO Guide, *supra* note 22.
36. GDPR Article 4(11).
37. GDPR Article 7(2). *See also* Recital 42.
38. Recital 32.
39. GDPR Article 7(3). Any processing that occurred pursuant to consent and before that consent was revoked remains valid, however. *Id.*
40. *See, e.g.,* Remarks by Assistant Attorney General for the Criminal Division Leslie R. Caldwell at the 22nd Annual Ethics and Compliance Conference, Oct. 1, 2014, https://www.justice.gov/opa/speech/remarks-assistant-attorney-general-criminal-division-leslie-r-caldwell-22nd-annual-ethics.
41. *See U.S. v. Microsoft Corp.*, No. 16-402, On Writ of Certiorari to The United States Court of Appeals for The Second Circuit. The question in this case is whether the DOJ can compel Microsoft to produce documents it has stored on servers in Ireland maintained by its Irish subsidiary.

Acknowledgment

The authors would like to acknowledge the assistance of their colleagues Bradford Hardin (counsel), Jacquelyn L. Stanley (senior associate), Zachary Goldman (senior associate), and Nicholas Simons (associate). The WilmerHale lawyers are members of the Regulatory and Government Affairs Department and the AML and Economic Sanctions Compliance and Enforcement practice.

Sharon Cohen Levin
WilmerHale
7 World Trade Center, 250 Greenwich Street
New York, New York 10007
USA

Tel: +1 212 230 8804
Email: sharon.levin@wilmerhale.com
URL: www.wilmerhale.com

Sharon Cohen Levin is a leading authority on anti-money laundering (AML), Bank Secrecy Act (BSA), economic sanctions and asset forfeiture. She served for 19 years as Chief of the Money Laundering and Asset Forfeiture Unit in the US Attorney's Office for the Southern District of New York (SDNY). Under her leadership, the SDNY forfeited in excess of $15 billion. During her tenure at SDNY, Ms. Levin prosecuted and supervised many of the Department of Justice's most complex and significant money laundering, sanctions and asset forfeiture prosecutions. Since joining WilmerHale she has represented a diverse array of financial institutions with respect to AML and sanctions issues, including developing AML and sanctions programs and counseling clients on AML and sanctions compliance. Ms. Levin represents individuals and institutions in criminal, civil and regulatory investigations and enforcement actions.

Ms. Cohen Levin's full professional profile is available at: https://www.wilmerhale.com/Sharon_Levin/.

Franca Harris Gutierrez
WilmerHale
1875 Pennsylvania Avenue
Washington, D.C. 20006
USA

Tel: +1 202 663 6557
Email: franca.gutierrez@wilmerhale.com
URL: www.wilmerhale.com

Franca Harris Gutierrez, a Partner and Vice Chair of the Financial Institutions Practice Group. Ms. Harris Gutierrez, who joined the firm from the US Department of the Treasury's Office of the Comptroller of the Currency (OCC), leads one of the country's preeminent banking and financial services practices. She advises clients on complex anti-money laundering issues arising in regulatory, enforcement, and transactional contexts. Maintaining an active enforcement practice, she defends clients before all the federal banking agencies and other federal and state enforcement bodies including the New York Department of Financial Services. She is a leader in a number of financial institutions spaces and counsels a broad range of US and non-US financial institutions.

Ms. Harris Gutierrez's full professional profile is available at: https://www.wilmerhale.com/franca_gutierrez/.

WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP ®

WilmerHale's interdisciplinary AML and Economic Sanctions Compliance and Enforcement Group brings together leading practitioners to focus on our clients' most challenging AML- and economic-sanctions-related regulatory, examination and enforcement issues. The team has a wealth of knowledge and government experience at the forefront of AML and sanctions policy and enforcement. Our lawyers have worked in the US Department of Justice, US Attorneys' Offices, the US Department of the Treasury, the US Department of State, the Central Intelligence Agency and the National Security Agency, the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the White House, and the United States Congress. This depth of experience enables us to assist clients in anticipating and understanding the government's priorities, communicating with regulators and key stakeholders, and resolving their most challenging matters and law enforcement proceedings.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com