Debevoise & Plimpton

FCPA Update
February 2021
Volume 12
Number 7

FCPA Update

A Global Anti-Corruption Newsletter

Also in this issue:

6 Deutsche Bank Resolves FCPA Investigation Regarding Business Development Consultants

Click here for an index of all FCPA Update articles

If there are additional individuals within your organization who would like to receive *FCPA Update*, please email prohlik@debevoise.com, eogrosz@debevoise.com, or pferenz@debevoise.com

An Update on the Impact of European Data Protection Laws When Responding to U.S. Government Requests

As covered in our June 2018 issue of *FCPA Update*,[1] European data protection laws[2] – most notably the EU General Data Protection Regulation ("GDPR") – present challenges for companies responding to U.S. government information requests. Then, the GDPR was in its infancy. Now, the enforcement agendas of many European Data Protection Authorities ("DPAs") have developed, and the risk of

Continued on page 2

1. Jeremy Feigelson, Jane Shvets, & Robert Maddox, "Impact of EU General Data Protection Regulation on Corporate Investigations and Due Diligence" FCPA Update, Vol. 9 No. 11 (June 2018), https://www.debevoise.com/insights/publications/2018/06/fcpa-june-2018.
2. "European data protection laws" refer to the laws of the European Economic Area and the United Kingdom that govern the use of personal data.

An Update on the Impact of European Data Protection Laws When Responding to U.S. Government Requests

Continued from page 1

civil claims for data protection violations is more concrete.[3] Below, we summarize the developments since June 2018 that may impact companies' consideration of European data protection compliance and cooperation with U.S. authorities' information requests.

I. A Refresher

Companies subject to European data protection laws have to comply with the following key obligations when responding to U.S. authorities' data requests:

- **Lawful basis**: Identifying and recording a "lawful basis" for processing personal data. The basis is often that the processing is in the company's "legitimate interests," which are not overridden by the fundamental rights of affected individuals.
- **Transparency**: Providing disclosures to affected individuals when complying with the U.S. authorities' requests, unless an exception under the GDPR or national law applies.
- **Data Minimization**: Ensuring that only personal data necessary to achieve the purpose of the processing is included.
- **Cross-border transfer restrictions**: Identifying and documenting a valid basis on which to transfer personal data from the European Economic Area ("EEA") or the UK to the United States. As covered in the June 2018 issue, the basis will often be the GDPR Article 49(1)(e) "derogation," which allows for cross-border transfers that are "necessary for the establishment, exercise or defence of legal claims."

II. Developments

Potential Challenges to Relying on "Legitimate Interests"

Influential but non-binding guidance issued in July 2019 highlights potential difficulties when relying on "legitimate interests" to process data for the purpose of complying with U.S. data requests. The European Data Protection Supervisor and European Data Protection Board ("EDPB") issued a joint legal opinion on the interaction between the GDPR and the U.S. CLOUD Act, the 2018 statute that expanded U.S. government's ability to obtain data from overseas.[4] The opinion reiterates the need for a two-stage legal analysis. *First*, identify the lawful basis for processing. *Second*, identify the ground for cross-border data transfer.

Continued on page 3

3. Jeremy Feigelson, Robert Maddox, et al., "European Data Protection Roundup: 2020 in Five Trends", Debevoise Data Blog (Jan. 21, 2021), https://www.debevoisedatablog.com/2021/01/21/european-data-protection-roundup-2020-in-five-trends/.

4. European Data Protection Board, "EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection" (July 12, 2019), https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

An Update on the Impact of European Data Protection Laws When Responding to U.S. Government Requests

Continued from page 2

Many companies have focused their analysis on the cross-border transfer issue. But the opinion highlights potential difficulties with relying on "legitimate interests" when responding to CLOUD Act requests. In particular, U.S. authorities' access to data under the CLOUD Act may create a risk of criminal liability in the U.S. for the individual targeted by the data request, creating a risk of dual criminality. This could override a company's legitimate interest in seeking to comply with a valid CLOUD Act request. Companies wanting to rely on "legitimate interests" may want to consider how the guidance impacts their balancing of the company's interests and individuals' rights when seeking to comply with a cross-border data request.

Public Interest Derogation: Another Avenue to Explore?

As covered on the Debevoise Data Blog[5], the UK Information Commissioner's Office ("ICO") recently published its letter to the U.S. Securities and Exchange Commission ("SEC") on the impact of the UK GDPR on UK-based SEC-regulated firms' ability to comply with SEC data requests. The ICO found that SEC-regulated UK firms can, in principle, transfer personal data to the SEC under the GDPR Article 49(1)(d) derogation for transfers that are "necessary for important reasons of public interest." The ICO relied on the fact that SEC oversight helps prevent financial crimes in the UK and that firms regulated by the UK Financial Conduction Authority ("FCA") must work with regulators globally in an open and cooperative manner under the FCA Handbook Principles for Businesses. While the ICO issued its opinion on the specific position of SEC-regulated UK firms and noted that it does not constitute "pan EU advice," companies may want to consider whether they can rely on the "public interest" derogation in other circumstances.

"Now, the enforcement agendas of many European Data Protection Authorities … have developed, and the risk of civil claims for data protection violations is more concrete."

Continued on page 4

5. Karolos Seeger, Jane Shvets, et al., "SEC Information Requests: UK Privacy Regulator Clarifies Position", Debevoise Data Blog (Feb. 8, 2021), https://www.debevoisedatablog.com/2021/02/08/sec-information-requests-ico-clarifies-position/.

Continued from page 3

Court Challenges

Since the GDPR came into force, individuals are more frequently enforcing their data protection rights through courts. Companies need to keep potential litigation risk in mind when considering data protection compliance in the context of U.S. data requests. For example, in May 2020, the Luxembourg Court of Appeal issued a preliminary order preventing the Luxembourg branch of a Swiss bank from transferring a customer's personal data to U.S. authorities after a petition from the customer to halt the transfer on data protection grounds.[6]

The question of whether the bank has a lawful basis for the cross-border transfer remains to be decided, but in the meantime the Swiss bank has to comply with the preliminary injunction or face a penalty of €100,000 per breach, up to a maximum of €1 million. The decision shows how individuals can use courts to prevent the transfer of their personal data to U.S. authorities. We expect to see more such cases in the future.

Redactions as a Route to Data Minimization

A company may have to engage with the U.S. requesting authority to explain how the GDPR data minimization obligations might affect the company's production.

In some cases, companies seek to discharge their data minimization obligations by redacting non-relevant personal data from transferred documents. Some U.S. courts have endorsed that approach. For example, in *SEC v. Telegram*, a judge in the U.S. District Court for the Southern District of New York issued an order that allowed Telegram to produce bank records "with redactions necessitated by foreign privacy laws and a log stating the basis for any redaction."[7] While decided on the case's specific facts, the *Telegram* order shows that non-U.S. privacy laws may sometimes justify redacting personal data. Companies may want to consider whether redactions are an appropriate way of meeting their data minimization obligations when responding to U.S. data requests.

Transparency-related Enforcement

European DPAs frequently issue fines against companies that fail to meet their transparency obligations in a wide variety of contexts, including internal investigations. For instance, the Hungarian DPA penalised a company for not informing an employee who was on long-term sick leave that their work files and emails were going to be processed in an investigation of potential misconduct.[8]

Continued on page 5

6. Arrêt N° 67/20 – VII – REF (May 6, 2020).
7. Order, *SEC v. Telegram*, No. 19-cv-9439 (S.D.N.Y. Jan. 13, 2020).
8. Resolution, no. NAIH/2019/769 (Oct. 15, 2019).

Continued from page 4

Companies should consider whether a GDPR-compliant data collection notice is warranted when conducting internal, or responding to government-led, investigations.

Data Protection Impact Assessments

Under the GDPR Article 35, companies have to perform a Data Protection Impact Assessment ("DPIA") in advance of data processing that is likely to result in a high risk to affected individuals' rights and freedoms. The GDPR requires DPAs to publish lists of circumstances in which a DPIA would be required. The list published by the French DPA, the CNIL, arguably covers internal investigations into alleged workplace misconduct. While it is not clear whether that would extend to compliance with U.S. authorities' data requests, companies should consider whether a DPIA may be required based on the local DPA guidance and the circumstances of the data request.

III. Conclusion

The European data protection landscape has developed since our June 2018 issue of *FCPA Update*, but our overarching view remains the same as then: data protection compliance need not and should not stop investigations and associated cross-border data transfers in their tracks. As the personal data risks and DPAs' expectations become clearer, companies should give careful consideration to data protection compliance when responding to data requests from U.S. authorities.

Karolos Seeger

Jane Shvets

Robert Maddox

Friedrich Popp

Karolos Seeger is a partner in the London office. Jane Shvets is a partner in the New York office. Robert Maddox is an associate in the London office. Friedrich Popp is an associate in the Frankfurt office. Full contact details for each author are available at www.debevoise.com.

Continued on page 6

Deutsche Bank Resolves FCPA Investigation Regarding Business Development Consultants

On January 8, 2021, Deutsche Bank AG agreed to pay more than $122 million to resolve DOJ and SEC investigations into alleged FCPA violations related to its dealings with business development consultants ("BDCs") in multiple jurisdictions.[1] Deutsche Bank entered into a three-year DPA with DOJ related to one count of conspiracy to violate the books and records and internal accounting controls provisions of the FCPA.[2] In particular, DOJ alleged that Deutsche Bank engaged in a scheme to maintain false books, records, and accounts to conceal payments to BDCs to facilitate bribery in order to obtain or retain clients over an approximately seven-year period. Under the DPA, Deutsche Bank will pay a criminal monetary penalty of more than $79 million relating to the FCPA conduct.[3] The SEC's cease-and-desist order similarly found that Deutsche Bank violated the books and records and internal accounting controls provisions, imposing disgorgement of $35 million with prejudgment interest of $8 million.[4]

The Abu Dhabi BDC

According to the U.S. agencies' filings in connection with the settlement, Deutsche Bank contracted with a BDC in Abu Dhabi around 2010 in order to obtain business with an investment vehicle indirectly owned by the government of Abu Dhabi.[5] At least four Deutsche Bank managing directors knew that the BDC was a relative of a high-ranking official for the investment vehicle and was acting as a proxy for that official, and that paying fees to the BDC was necessary to obtain business from the investment vehicle. Deutsche Bank's Global Markets Risk Assessment Committee approved the bank's engagement with the BDC despite certain indicia of potential corruption risk, including: (1) the BDC's relationship to government officials; (2) the BDC's lack of qualifications; (3) the indirect involvement of another intermediary – a relative of the BDC and also business partner of the high-ranking

Continued on page 7

1. U.S. Dep't of Justice, "Deutsche Bank Agrees to Pay over $130 Million to Resolve Foreign Corrupt Practices Act and Fraud Case," Press Release No. 21-23 (Jan. 8, 2021), https://www.justice.gov/opa/pr/deutsche-bank-agrees-pay-over-130-million-resolve-foreign-corrupt-practices-act-and-fraud; Deferred Prosecution Agreement, *United States v. Deutsche Bank Aktiengesellshaft*, No. 20-584 (E.D.N.Y. Jan. 8, 2021), https://www.justice.gov/opa/press-release/file/1360741/download (hereinafter "Deutsche Bank DPA"); Information, *United States v. Deutsche Bank Aktiengesellshaft*, No. 20-584 (E.D.N.Y. Jan. 8, 2021), https://www.justice.gov/opa/press-release/file/1351746/download (hereinafter "Deutsche Bank Information"); Order, *In re Deutsche Bank AG*, Securities Exchange Act Rel. No 90875 (Jan. 8, 2021), https://www.sec.gov/litigation/admin/2021/34-90875.pdf (hereinafter "SEC Order").
2. Deutsche Bank DPA ¶¶ 2, 3.
3. *Id.* ¶ 4. Deutsche Bank will also pay a criminal monetary penalty of more than $5.5 million relating to commodities trading conduct. *Id.*
4. SEC Order ¶¶ 2, 42.
5. Deutsche Bank DPA ¶¶ 9-22; Deutsche Bank Information ¶¶ 12-25; SEC Order ¶¶ 17-23.

Deutsche Bank Resolves FCPA Investigation Regarding Business Development Consultants

Continued from page 6

official for the investment vehicle – who had roles with several state-owned entities; and (4) pressure from the official for the investment vehicle to finance a yacht in which he had an ownership interest.

Deutsche Bank ultimately financed the yacht. It also engaged the BDC prior to conducting any due diligence or documenting the BDC's full name. That engagement included a success fee of €1.5 million and a monthly retainer of €85,000. In total, Deutsche Bank paid the Abu Dhabi BDC more than €3.4 million, without any invoices and with minimal evidence of services provided.

The Saudi BDC

The U.S. agencies also alleged that Deutsche Bank entered into a BDC contract around 2011 with a special purpose vehicle ("SPV") beneficially owned by the wife of an individual responsible for managing the family office of a Saudi official.[6] Deutsche Bank paid the SPV fees falsely recorded as "referral fees," when in fact they were to retain the family office's business. In return, Deutsche Bank managed hundreds of millions of dollars in investments for the family office.

At least four managing directors of Deutsche Bank and several other high-level employees knew that the purpose of engaging the Saudi BDC was to bribe the family office manager. One Deutsche Bank director falsely portrayed in internal documentation the BDC as the source of the business with the family office. Deutsche Bank made four payments to the BDC totaling more than $1,000,000 and provided the family office manager with additional benefits including a €635,000 loan to purchase a house in France.

The Italian BDC

According to the U.S. agencies' filings, Deutsche Bank also entered into a BDC relationship around 2007 with a regional tax judge to bring clients to Deutsche Bank.[7] Deutsche Bank managing directors and employees submitted false invoices and records of payments to this BDC, including multiple payments for the same services or payments for no services at all. When some invoices were challenged, a Deutsche Bank director falsely linked the introduction of three accounts to the BDC.

In a later year, the BDC demanded more money than entitled to under his contract. In response, Deutsche Bank agreed to find additional work for the BDC. Although the BDC later provided some research materials, email communications show that the payment was not for the materials submitted. In sum, Deutsche Bank paid the BDC more than $850,000.

Continued on page 8

6. Deutsche Bank DPA ¶¶ 23-36; Deutsche Bank Information ¶¶ 26-39.

7. Deutsche Bank DPA ¶¶ 37-41; Deutsche Bank Information ¶¶ 40-44; SEC Order ¶¶ 24-27.

Deutsche Bank Resolves FCPA Investigation Regarding Business Development Consultants
Continued from page 7

Conclusion

These DOJ and SEC resolutions are the latest matters that Deutsche Bank has resolved with U.S. enforcement authorities and place it on the list of FCPA recidivists. In 2015, Deutsche Bank paid $775 million in criminal penalties to DOJ in connection with its role in manipulating LIBOR.[8] In 2017, it paid $7.2 billion to resolve federal civil claims that it misled investors as to residential mortgage-backed securities in 2006 and 2007.[9] And in 2019, it paid $16 million to the SEC to settle FCPA claims related to its hiring of relatives of public officials in China and Russia.[10]

More broadly, Deutsche Bank's recent FCPA settlements underscore, once again, the compliance risks posed by third-party consultants retained to obtain business, particularly from state-owned or state-controlled entities.

Andrew M. Levine

Winston M. Paes

Matthew Specht

Andrew M. Levine and Winston Paes are partners in the New York office. Matthew Specht is an associate in the New York office. Full contact details for each author are available at www.debevoise.com.

8. U.S. Dep't of Justice, "Deutsche Bank's London Subsidiary Agrees to Plead Guilty in Connection with Long-Running Manipulation of LIBOR," Press Release No. 15-499 (Apr. 23, 2015), https://www.justice.gov/opa/pr/deutsche-banks-london-subsidiary-agrees-plead-guilty-connection-long-running-manipulation.
9. U.S. Dep't of Justice, "Deutsche Bank Agrees to Pay $7.2 Billion for Misleading Investors in its Sale of Residential Mortgage-Backed Securities," Press Release No. 17-077 (Jan. 17, 2017), https://www.justice.gov/opa/pr/deutsche-bank-agrees-pay-72-billion-misleading-investors-its-sale-residential-mortgage-backed.
10. U.S. Securities & Exchange Commission, "SEC Charges Deutsche Bank with FCPA Violations Related to Its Hiring Practices" (Aug. 22, 2019), https://www.sec.gov/enforce/34-86740-s.

FCPA Update

FCPA Update is a publication of
Debevoise & Plimpton LLP

919 Third Avenue
New York, New York 10022
+1 212 909 6000
www.debevoise.com

Washington, D.C.
+1 202 383 8000

London
+44 20 7786 9000

Paris
+33 1 40 73 12 12

Frankfurt
+49 69 2097 5000

Moscow
+7 495 956 3858

Hong Kong
+852 2160 9800

Shanghai
+86 21 5047 1800

Tokyo
+81 3 4570 6680

Luxembourg
+352 27 33 54 00

Bruce E. Yannett
Co-Editor-in-Chief
+1 212 909 6495
beyannett@debevoise.com

Andrew J. Ceresney
Co-Editor-in-Chief
+1 212 909 6947
aceresney@debevoise.com

David A. O'Neil
Co-Editor-in-Chief
+1 202 383 8040
daoneil@debevoise.com

Jane Shvets
Co-Editor-in-Chief
+44 20 7786 9163
jshvets@debevoise.com

Philip Rohlik
Co-Executive Editor
+852 2160 9856
prohlik@debevoise.com

Kara Brockmeyer
Co-Editor-in-Chief
+1 202 383 8120
kbrockmeyer@debevoise.com

Andrew M. Levine
Co-Editor-in-Chief
+1 212 909 6069
amlevine@debevoise.com

Karolos Seeger
Co-Editor-in-Chief
+44 20 7786 9042
kseeger@debevoise.com

Erich O. Grosz
Co-Executive Editor
+1 212 909 6808
eogrosz@debevoise.com

Andreas A. Glimenakis
Associate Editor
+1 202 383 8138
aaglimen@debevoise.com

Please address inquiries regarding topics covered in this publication to the editors.

Please note:
The URLs in *FCPA Update* are provided with hyperlinks so as to enable readers to gain easy access to cited materials.