International
Comparative
Legal Guides

Practical cross-border insights into sanctions

Sanctions 2022

Third Edition

Contributing Editors:
Roberto J. Gonzalez & Rachel M. Fiorill
Paul, Weiss, Rifkind, Wharton & Garrison LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Germany


Michael Walther
Gibson, Dunn & Crutcher LLP


Richard Roeder
Gibson, Dunn & Crutcher LLP


Meribeth Banaschik
EY Forensic & Integrity Services


Bisman Sethi
EY Forensic & Integrity Services

Gibson, Dunn & Crutcher LLP
EY Forensic & Integrity Services

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

Germany applies all sanctions imposed by the United Nations Security Council ("**UNSC**") ("**UN Sanctions**") and, as a European Union ("**EU**") Member State, all sanctions are imposed by the EU ("**EU Sanctions**").

Germany does not unilaterally impose sanctions. However, Germany maintains a discrete national export control regime that – in very limited circumstances – is used to impose unilateral export control measures that are sometimes referred to as "German Sanctions" externally. For details, please refer to question 2.10 below.

Germany's sanctions regime distinguishes between sanctions with a focus on a specific jurisdiction ("*Länderbezogene Embargomaßnahmen*") and sanctions with a focus on specific individuals/entities ("*Personenbezogene Embargomaßnahmen*"). In the following, we shall refer to both as "*sanctions*" and use the terminology explained below.

Sanctions with a focus on a specific jurisdiction can further be divided into (full) embargoes, comprehensive sanctions and targeted sanctions. Embargoes, as the term is used herein thereafter, prohibit all trade with or for the benefit of the sanctioned party. Comprehensive sanctions prohibit most forms of trade with or for the benefit of the sanctioned party. Targeted sanctions prohibit only specific forms of trade with or for the benefit of the sanctioned party.

Embargoes and comprehensive sanctions are regularly implemented in the form of economic sanctions. Targeted sanctions may also be implemented in the form of economic sanctions but more often than not, are implemented in the form of financial sanctions.

Economic sanctions, broadly comparable to U.S. sectoral sanctions, are designed to restrict trade, usually within a particular economic sector, industry or market – *e.g.*, the oil and gas sector or the defence industry ("**Economic Sanctions**").

Financial Sanctions, broadly comparable to U.S. Specially Designated Nationals ("**SDN**") listings, are restrictive measures taken against specific individuals or entities that may originate from a sanctioned country or may have committed a condemned activity ("**Financial Sanctions**").

These natural persons and organisations are identified and listed by the EU in the EU Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions ("**EU Consolidated List**") (see question 2.4 below for details), resulting in targeted restrictions. With the application of EU Financial Sanctions, all funds and economic resources belonging to, owned by, held by or controlled by natural or legal persons, entities and bodies listed are frozen. Moreover, no funds or economic resources can be made available, directly or indirectly, to or for the benefit of the listed parties. Finally, the knowing and intentional participation in activities intended to circumvent the EU Sanctions is also prohibited.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

The government agencies that administer or enforce EU Sanctions and the German export control regime in Germany are:

(i) the German Federal Bank ("*Deutsche Bundesbank*"), the competent authority for administering Financial Sanctions;
(ii) the Federal Office for Economic Affairs and Export Controls ("*Bundesamt für Wirtschaft und Ausfuhrkontrolle*" ("**BAFA**")), the competent authority for administering Economic Sanctions and the export control regime;
(iii) the Public Prosecutor's Office ("*Staatsanwaltschaft*"), the competent authority to enforce breaches of sanctions amounting to a crime; and
(iv) the German Customs Administration ("*Zoll*"), the competent authority to, *inter alia*, enforce breaches of sanctions that constitute an administrative offence.

Furthermore, the Federal Office for the Protection of the Constitution ("*Bundesamt für Verfassungsschutz*") ("**BfV**"), in close cooperation with the domestic intelligence services of the German federal states and with other agencies, including BAFA, is responsible for uncovering any activities of proliferation concern in order to prevent any illegal procurement efforts of foreign countries. Also, the Financial Intelligence Unit ("**FIU**"), the central office for financial transaction investigations, organised as part of to the German Customs Administration system, analyses suspicious activity reports under the Money Laundering Act, that include the overlapping topic of terrorist financing.

Finally, the EU Commission is the competent authority for certain sanctions-related authorisation requests.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

Yes.

The EU has introduced further EU Sanctions, both Economic Sanctions and Financial Sanctions, against those deemed to be responsible for, *inter alia*, the crackdown by Belarusian security forces on protesters, democratic opposition and journalists.

Further, on December 7, 2020, the EU established the EU's first global and comprehensive human rights sanctions regime ("**EU Human Rights Sanctions**").

The EU Human Rights Sanctions allow the EU to target individuals and entities responsible for, involved in or associated with serious human rights violations and abuses, and provides for the possibility to impose travel bans, asset freeze measures and the prohibition of making funds or economic resources available to those designated.

One noteworthy case law, the German Federal Court of Justice ("*Bundesgerichtshof*") ("*BGH*") decided on August 31, 2020, that the procurement of materials for a foreign intelligence service, while circumventing EU Sanctions, fulfils the elements of a crime under section 18 para. 7 No. 1 of the Foreign Trade and Payments Act ("*Außenwirtschaftsgesetz*") ("*AWG*"). Espionage or affiliation with an intelligence service is not necessary to act "*for the intelligence service of a foreign power*".

In the case, a man sold machine tools to Russian companies for around EUR 8 million in seven cases between 2016 and 2018. The man's actual contractual partner – a member of a Russian intelligence service – subsequently supplied the machines to a Russian state-owned arms company for military use. The arms company operates in the field of carrier technology and develops cruise missiles. The machine tools are considered dual-use technology, and the sale and export of such items to Russia has been prohibited since 2014 under the EU Russia Sanctions, specifically Regulation (EU) 883/2014 as amended.

The BGH decided that it is sufficient if the delivery of the machines is a result of the perpetrator's involvement in the procurement structure of foreign intelligence services. An organisational integration of the perpetrator into the foreign intelligence service is not required to justify the higher penalty of section 18 para. 7 No. 1 AWG (imprisonment of not less than one year) compared to the regular sentencing range of section 18 para. 1 AWG (imprisonment from three months up to five years) imposed for embargo violations under the AWG.

Regarding the discussion around the extraterritorial U.S. sanctions against the Nord Stream II project and the European and specifically the German reaction to it, a recent agreement between the U.S. and Germany eased respective tensions.

At the same time, the broader discussion on defending the EU's and Germany's sovereignty, specifically on foreign policy and trade-related issues remains prevalent, as a recent respective study of the European Parliament shows. Specifically, on January 19, 2021, the EU Commission published a Communication to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions titled "*The European economic and financial system: fostering openness, strength and resilience*" as a "*key instrument*" playing a "*critical role in upholding the EU's values and in projecting its influence internationally*".

Following-up on the above, the EU Commission now announced that "*it would consider amending the Blocking Statute (Regulation 2271/96), to further deter and counteract the unlawful extra-territorial application of sanctions to EU operators by countries outside the EU.*" In such announcement, the EU Commission included what it could envisage, stating, *inter alia*: *"(…) the proposed regulation could envisage the award of financial or other types of support to EU operators willing to engage in trade that is prohibited by such extra-territorial sanctions of third countries but not prohibited by Union law(…).*"

2 Legal Basis / Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

Germany does not unilaterally impose sanctions, but applies all UN and EU Sanctions, see question 1.1 above.

The legal authority for EU Sanctions is article 29 of the Treaty on the EU ("**TEU**") (in the case of arms embargoes) and article 215 of the TEU (in the case of Economic and Financial Sanctions).

In the case of arms embargoes, the Council of the EU (the "**Council**"), the institution representing the governments of the EU Member States, adopts a respective decision as part of its Common Foreign and Security Policy ("**CFSP**"). This decision is binding on EU Member States, which, in turn, implement the decision on an EU Member State level. In Germany, the legal authority for such implementation and enforcement is the Foreign Trade and Payments Act ("**AWG**"), flanked by the administrative authority, the Foreign Trade and Payments Regulation ("**AWV**").

In the case of EU Economic Sanctions and EU Financial Sanctions, the Council again adopts a respective decision as part of its CFSP and, additionally, an EU Sanctions regulation which is directly applicable in all EU Member States. While the EU Member States thus do not need to implement such EU Sanctions regulations in national EU Member State law, the EU Sanctions regulations require the EU Member States to create authorities to assure enforcement of the EU regulation on an EU Member State level.

Regarding the legal authorities or administrative authorities for implementing UN sanctions, please see question 2.2 below.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Yes.

United Nations ("**UN**") Sanctions are regularly implemented via EU Sanctions that in turn apply in Germany, see question 2.1 above.

As the process of the implementation of UN Sanctions via EU Sanctions may cause a delay between listing by the UN and applicability in Germany, Germany additionally directly implements UN Sanctions based on section 6 para. 1 AWG in connection with section 4 para. 1 No. 2 and 3 AWG in connection with section 4 para. 2 No. 3 AWG and section 13 para. 6 AWG.

There are no significant ways in which the EU and/or Germany have failed to implement UN Sanctions.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

Yes.

Germany is a Member State of the EU and implements EU sanctions, see question 2.1 above. Regarding the process of implementation in the case of arms embargoes, EU Economic Sanctions and EU Financial Sanctions, the Council adopts a respective decision as part of CFSP. In Germany, the legal basis for implementation into German law and respective enforcement of such decision is the AWG, flanked by the administrative authority AWV.

In the case of EU Economic Sanctions and EU Financial Sanctions, the respective additional EU Sanctions regulation is directly applicable in all EU Member States. Therefore, while the EU Member States do not need to implement such EU Sanctions regulations in national EU Member State law, the EU Sanctions regulations require EU Member States to implement authorities to assure enforcement of the EU regulation on an EU Member State level, in Germany via the AWG, flanked by the administrative authority AWV.

There are no significant ways in which Germany has failed to implement EU Sanctions.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Germany does not maintain a list of sanctioned individuals and entities, but applies the EU Consolidated List. For the process of the implementation of such EU Financial Sanctions, see questions 2.1 and 2.3 above; for further details on (de-)listing, see https://www.consilium.europa.eu/en/policies/sanctions/adoption-review-procedure/.

Individuals and entities are added to or removed from the EU Consolidated List upon a proposal of the High Representative of the EU for Foreign Affairs or an EU Member State. Various bodies and committees of the Council discuss the respective proposal before the Council decides on the addition/removal by unanimous vote.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

Sanctioned persons may submit a request to the Council, asking for the reassessment of the listing decision (see here for details: https://www.consilium.europa.eu/en/policies/sanctions/adoption-review-procedure/).

According to articles 275 and 263 of the Treaty of the Functioning of the EU, sanctioned persons may also challenge the Council's listing decision before the EU General Court of the European Union.

The European Court of Justice ("**ECJ**") may also review whether UNSC Sanctions, specifically those related to listings, are in accordance with EU primary law. For illustration purposes, a respective judgment can be found at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62005CJ0402&from=DE.

2.6 How does the public access those lists?

The sanctions search tool maintained by the EU, the so-called "**EU Sanctions Map**" (available at https://www.sanctionsmap.eu), serves as a good starting point for an initial assessment on whether Germany maintains sanctions against a particular jurisdiction, individual or entity.

An overview of sanctions with a focus on specific jurisdictions can be found at https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_embargo_uebersicht_laenderbezogene_embargos.pdf?__blob=publicationFile&v=6.

An overview of sanctions with a focus on specific individuals/entities, the so-called EU Consolidated List of persons, groups and entities subject to EU Financial Sanctions, can be found at https://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions. Accessing search links however, from a Business As Usual ("**BAU**") standpoint can be a cumbersome task, especially as sanctions screening should be performed at both the onboarding phase of a transaction or relationship, and should also continue to be monitored throughout the relationship cycle. Therefore, most companies often rely on external vendors and third parties with compliance expertise, to provide leading technology led screening solutions. The integration of sanctions screening solutions that combine technology and advanced analytics can facilitate faster screening and monitoring for review and reporting requirements.

How can companies manage those lists?

Companies often must rely on external vendors and third parties with compliance expertise to provide leading technology and screening solutions. Sanctions screening should be performed at the onboarding phase of a transaction or relationship, and ongoing monitoring should continue throughout the relationship cycle. While screening at the onboarding stage appears straightforward, one of the key challenges can be adopting an automated screening system integrated with the organisation's onboarding systems including, *inter alia*, Enterprise Resource Planning ("**ERP**"), Customer Relationship Management ("**CRM**") and Human Resources ("**HR**") systems. The integration of screening solutions that combine technology and advanced analytics can facilitate faster screening and monitoring for review and reporting requirements.

What does ongoing monitoring involve and what is its relevance to businesses?

Ongoing monitoring includes a review of an organisation's relevant key data sets against any new updates to the sanctions watch lists. Ongoing monitoring ensures that business activities are up to date and in line with the risk assessment conducted at the time of onboarding. Many companies automate this procedure, to check for changes in politically exposed person ("**PEP**") status, penalties, and negative publicity on a regular basis. They monitor any changes in customer risk and exposure by screening against dynamic, up-to-date global databases. This process also takes into consideration records where key know-your-customer ("**KYC**") attributes such as address, nationality and other personal identification indicators may have been updated as a part of the organisation's anti-money laundering ("**AML**") KYC refresh regime.

The global economic and financial landscape has shifted dramatically as a result of the COVID-19 pandemic. On one hand, increased unemployment has prompted unscrupulous actors to commit financial crime through charity organisations, digital e-wallet platforms and cryptocurrency exchanges, exposing businesses to a higher risk of money laundering and terrorist financing creating the need for a more robust ongoing monitoring framework. While most screening systems and solutions today support automated ongoing review requirements, there is significant operational optimisation that can be achieved through effective technology system configurations. This includes review and mapping of the organisation's data with the corresponding data available in the watch lists. A well-tuned technology solution will assist the organisation in reviewing potential matches through a framework that can support internal system integrations and real-time triggers based on automated watch lists updates.

Automated ongoing monitoring can assist businesses with monitoring the risk profiles of their customers and third parties, while not changing in a way that exposes the firm to non-compliance and reputation damage. Organisations greatly benefit from conducting ongoing risk assessment of their business relationships, which include the primary engaging entity ("customer" and or "third party"), its ultimate beneficiary ownership ("**UBO**") and senior management ("**SM**") officials. The primary customer along with the key associations (UBOs and SMs) are then reviewed on a watch list, belonging to a sanctioned country or a high-risk industry.

What causes higher false positives and how can how can organisations manage false positives better?

One of the top reasons of higher false positives is continued reliance on rule-based screening engines. While technology for name screening evolves rapidly, the issue of false positives is still

seen as one of the top challenges organisations face to accurately detect true screening matches. It is observed in most legacy systems that screening rules are built to scan customer data fields, not available on the watch list dataset. This would include running screening rules in combination with data such as date of birth, address, and passport information. This, however, can benefit only to the extent that this information is available on the watch list dataset, which unfortunately is not the case for a large percentage of records in the watch list data, resulting in higher false positives, due to the missing variable elements.

Another leading reason for increased false positives is the quality of data used for the screening. It is observed that the gaps in the data capture design requirements, which increases the chances of errors in the data capture process, and can therefore increase the risk of false positives and false negatives occurring.

Many advanced screening solutions offer capabilities based on nautral language processing ("**NLP**") technologies in machine learning to optimise false positives. The NLP technology assists organisations to read unstructured data and determine its meaning in the screening process. Organisations are now looking at a hybrid approach to achieve enhanced false positive optimisation. The hybrid approach includes technology functions that optimise the potential matches based on variations in word boundaries, native character variations (such as "ö" to "oe"), extra words or spelling errors in commonly found names, which are often caused by unintentional error(s) or introduced intentionally to evade detection. Advanced screening tools also use a combination of match screening algorithms that are tuned using the organisations historical, manually conducted false positive screening reviews. Another functionality that can assist organisations to optimise false positives is effective "whitelisting". This feature can allow organisations to list entities that could be exempted from the screening process.

False positive optimisation is increasingly important as it can help manage customer onboarding and transaction experience, without compromising on the effectiveness of the AML compliance requirements. Effective management of false positive matches may also reduce the likelihood of breaching other areas of law such as the principle of data minimisation or data accuracy in article 5 of the EU General Data Protection Regulation ("**GDPR**").

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

For an explanation of the different types of sanctions, please see question 1.1.

The UN, the EU and, correspondingly, Germany currently do not apply embargoes against any country or region.

However, North Korea is currently subject to comprehensive sanctions and the Crimea Region is currently subject to a broad set of targeted sanctions.

2.8 Does your jurisdiction maintain any other sanctions?

Germany, as of August 11, 2021, applies sanctions targeting CFSP concerns specifically related to 33 non-EU countries: Afghanistan; Belarus; Bosnia and Herzegovina; Burundi; Central African Republic; China; Democratic Republic of the Congo; Guinea; Guinea-Bissau; Haiti; Iran; Iraq; Lebanon; Libya; Mali; Moldova; Montenegro; Myanmar (Burma); Nicaragua; North Korea; Russia; Serbia; Somalia; South Sudan; Sudan; Syria; Tunisia; Turkey; Ukraine; United States; Venezuela; Yemen; and Zimbabwe.

2.9 What is the process for lifting sanctions?

The same procedure for the imposition of sanctions applies to the revocation of sanctions; please refer to question 2.1 above.

Accordingly, the decision by the Council must also be unanimous. This requirement has led to the fact that EU Sanctions regulations often contain an end date, so that instead of a uniform decision to lift them, a uniform decision to maintain the sanctions will usually be required every six months.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Yes.

Germany maintains a discrete and complex national export control regime. The German export control regime is regulated by the AWG. The AWV governs both the transfer to EU Member States and the export to non-EU Member States of certain goods.

The German export control regime implements requirements from the relevant international agreements, such as the Wassenaar Arrangement, the Nuclear Suppliers Group, the Australian Group and the Missile Technology Control Regime. It is a discrete national regime, yet Germany regularly aligns with the CFSP, specifically via the EU Dual Use Regulation and the EU Common Military List.

On the EU Dual Use Regulation, in order to keep up with the latest technological developments and to mitigate national security concerns, on May 10, 2021, the Council of the EU adopted a regulation that, by recasting Council Regulation (EC) No. 428/2009 (the "***EU Dual-Use Regulation***"), not only modernises, but also substantially expands the scope and breadth of the EU system for the control of exports, brokering, technical assistance, transit and transfer of dual-use products and technologies (the "***New EU Dual-Use Regulation***").

The New EU Dual-Use Regulation will: (i) strengthen controls on a wider range of emerging dual-use technologies, including cyber-surveillance tools, that can be used for both civilian and military applications; (ii) introduce due diligence obligations and compliance requirements for exporters, recognising the role of the private sector in addressing the risks posed by trade in dual-use items to international security; and (iii) increase the coordination between Member States and the EU Commission in support of the effective enforcement of controls throughout the EU.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

Yes.

Germany enforces the EU Blocking Statute (as amended, the "**EU Blocking Statute**"), and the AWV also includes the prohibition against declaring adherence to a foreign boycott. Further, the GDPR, while having the primary function of protecting the personal data and privacy rights of EU data subjects in practice, can sometimes act as a "Blocking Statute" prohibiting transfers to non-EEA countries or the processing of personal data pursuant to obligations that arise outside of EU or EU Member State law.

EU Blocking Statute

On August 6, 2018, the EU enacted Commission Delegated Regulation (EU) 2018/1100, which amended Council Regulation

(EC) No. 2271/96. The effect of the EU Blocking Statute is to prohibit compliance by EU entities with, *inter alia*, the re-imposed U.S. sanctions on Iran as well as certain U.S. sanctions on Cuba, most relevant are those deriving from the application of certain parts of the U.S. Cuban Liberty and Democratic Solidarity Act of 1996, the so-called "Helms-Burton Act".

The EU Blocking Statute was originally enacted in 1996 as a countermeasure to certain U.S. extraterritorial sanctions against Cuba, Iran and Libya. The EU viewed these sanctions as a violation of international law, a threat to international trade, and an impairment of the interests of "EU Operators". Consequently, pursuant to its preamble, the regulation sought to protect against the "*effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom*". To achieve that goal, the statute, *inter alia*, prohibits compliance with any legal acts listed in the regulation which "*purport to regulate activities of natural or legal persons under the jurisdiction of a Member State*". The Member States of the EU are responsible for implementing sanctions to be imposed in the event of a breach. Germany does so by penalising a breach of the EU Blocking Statute as an administrative offence with a maximum fine of EUR 500,000 with the potential of additional forfeit of gains.

In addition, the EU Blocking Statute nullifies the effect of foreign court judgments based on these legal acts in the EU, hinders service and discovery requests, such as those deriving from Helms-Burton Act claims and establishes a reporting obligation as well as a right to recover damages. These effects and obligations have been discussed in depth at https://www.gibsondunn.com/new-iran-e-o-and-new-eu-blocking-statute-navigating-the-divide-for-international-business/.

Boycott Declaration Prohibition

Section 7 of the AWV states: "*The issuing of a declaration in foreign trade and payments transactions whereby a resident participates in a boycott against another country (boycott declaration) shall be prohibited (…).*"

There is no precedent clarifying the exact scope, but it is a common understanding among sanctions practitioners in Germany that, unlike the EU Blocking Statute, section 7 of the AWV does not prohibit mere compliance with foreign sanctions; rather, it specifically prohibits the *issuing of a declaration* to do so.

On December 19, 2018, section 7 of the AWV was amended, clarifying that "[*The boycott declaration prohibition] shall not apply to a declaration that is made in order to fulfil the requirements of an economic sanction by one state against another state against which the Security Council of the United Nations in accordance with Chapter VII of the United Nations Charter, the Council of the European Union in the context of Chapter 2 of the Treaty on European Union or the Federal Republic of Germany has also imposed economic sanctions*".

This revision only leaves a narrow window of application of section 7 of the AWV. As an example, due to no UN, EU and, accordingly, German Sanctions implemented or applied against Cuba, the issuing of a boycott declaration relating to Cuba in the context with a German nexus should be approached carefully.

General Data Protection Regulation

Sanctions screening involves screening customer data against designated sanction lists. The very act of inputting a name (or, indeed, other details such as address, nationality, passport, tax ID, place of birth, date of birth, former names and aliases) into a sanctions screening tool or the filing of a Suspicious Activity Report ("**SAR**") could qualify as an act of personal data processing under the GDPR.

The processing of personal data is lawful under the GDPR when conducted in line with one of the legal bases provided in the regulation, such as when it is "(…) *necessary for compliance with a legal obligation to which the controller is subject (…)*" as per article 6(1)(c) of the GDPR. While a German company may be able to rely on EU sanctions law as a "*legal obligation*" justifying the screening of personal data under some circumstances, this may not necessarily be the case for sanctions screening due to U.S. and other third-country sanctions, export control laws and regulations – which stems from a "*legal obligation*" arising outside of EU or EU Member State law.

Further, the "*Schrems II*" judgment (CJEU Case C-311/18) on July 16, 2020 invalidated the EU-US Privacy Shield and consequently put into doubt the legality of personal data transfers to the United States without additional safeguards. However, for now, personal data that is transferred to courts, tribunals, and administrative authorities outside the EEA (pursuant to a mutual legal assistance treaty or equivalent) or under an article 49 GDPR derogation do not seem to be affected by the judgment. In practice what this means is that German companies should continue to monitor this area of the law for potential developments.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as "Secondary Sanctions")?

No, however, please note that EU Sanctions regularly apply to businesses carried out in whole or in part in the EU.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

Broadly speaking, any parties and transactions with a nexus to Germany and/or the EU may be subject to sanctions as well as export control laws and regulations applicable in Germany.

In Germany specifically, any trade in goods, services, capital, payments and other types of trade with foreign (*i.e.*, non-German) territories, as well as the trade in foreign valuables and gold between residents of Germany ("*Außenwirtschaftsverkehr*"), while not restricted *per se*, is subject to Germany's sanctions and export control laws and regulations, specifically to the restrictions of the AWG and AWV.

This also includes restrictions of international agreements, which the German legislative bodies have approved in the form of federal acts, such as the Wassenaar Arrangement, the Nuclear Suppliers Group, the Australian Group and Missile Technology Control Regime, and legal provisions of the bodies of international organisations to which the Federal Republic of Germany has transferred sovereign rights (*i.e.*, the EU).

EU Sanctions, in turn, generally apply: (i) within the territory of the EU; (ii) on board any aircraft or vessel under the jurisdiction of an EU Member State; (iii) to any person inside or outside the territory of the EU who is a national of an EU Member State; (iv) to any legal person, entity or body, inside or outside the territory of the EU, which is incorporated or constituted under the law of an EU Member State; and (v) to any legal person, entity or body in respect of any business done in whole or in part within the Union (for more information, please refer to the factsheet for EU restrictive measures, available at https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/135804.pdf).

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Yes.

Any individual or entity obliged to comply with EU Financial Sanctions, regularly EU banks and financial institutions, that know or have reasonable cause to suspect that they are in control or in possession of, or are otherwise dealing with, the funds or economic resources of a person subject to EU Financial Sanctions, must (i) freeze the funds and specifically not deal with them or make them available to, or for the benefit of, the designated person, and (ii) report the funds or economic resources to the competent authority of the EU Member State (in Germany, the Federal Bank). See question 3.4 for further details on reporting.

Making payments to a bank account of a sanctioned person is prohibited, unless specifically authorised by competent authority or unless it is reasonably determined that the funds will not be made available to the sanction person. EU banks may credit frozen accounts insofar it can be ascertained that the incoming funds are frozen upon being credited to the account.

For specific questions on freezing of funds and/or making available economic resources, please see the respective Commission opinion of June 19, 2020, available at https://ec.europa.eu/info/sites/info/files/200619-opinion-financial-sanctions_en.pdf.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

Yes.

For EU Financial Sanctions, *e.g.*, based on *Council Regulation (EU) 269/2014 of March 17, 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine* as amended, the competent authorities of the EU Member State to enforce such EU Financial Sanctions (in Germany, the Federal Bank) may authorise the release of certain frozen funds or economic resources, or the making available of certain funds or economic resources, after having determined that the funds or economic resources concerned are necessary to satisfy the basic needs of the sanctioned person or if the funds or economic resources concerned are intended exclusively for payment of reasonable professional fees or reimbursement of incurred expenses associated with the provision of legal services.

For EU Economic Sanctions, *e.g.*, based on *Council Regulation (EU) 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine* as amended, the competent authorities of the EU Member State to enforce such EU Economic Sanctions (in Germany, BAFA) may authorise certain transactions, *e.g.*, the sale of certain items for use in Russia used for oil exploration and production in waters deeper than 150 metres.

For specific licences related to the EU Blocking Statute, the respective request should be sent to the EU Commission's dedicated EU Blocking Statute team at: EC-AUTHORISATIONS-BLOCKING-REG@ec.europa.eu.

The German export control regime also includes exceptions and authorisation requirements. A more detailed description on the respective process can be found at https://www.bafa.de/EN/Foreign_Trade/Export_Control/export_control_node.html.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

Yes.

According to the respective provisions of EU Financial Sanctions, *e.g.*, *Council Regulation (EU) 269/2014 of March 17, 2014*, those who are subject to EU Financial Sanctions must: supply immediately any information which would facilitate compliance with the Regulation to the competent authority of the EU Member State authority, in Germany accordingly, to the Federal Bank; must transmit such information to the EU Commission; and must cooperate with the competent authority.

Further, there are additional reporting obligations in place, e.g., financial institutions, traders of goods, notaries, lawyers, auditors, tax consultants and real estate professionals are all required to report suspicious activities and transactions. Such organisations are expected to report information about sanctioned individuals through reporting of SARs, or Suspicious Activity Reports. These must be reported to the Deutsche Bundesbank, which is responsible for the implementation of EU Regulations on Financial Sanctions in Germany, and/or the FIU. Specifically, in case of asset freezes due to EU Financial Sanctions, banks and financial institutions must provide information about any funds, accounts, assets, BIC codes, reference numbers, amounts and dates connected with the sanctioned individuals and entities.

How can technology support regulatory reporting?

Advanced screening tools can facilitate automated regulatory reporting. The identified suspicious sanctions activity is reviewed through a case management workflow. Once the required information is consolidated and review remarks are updated, the system enables consolidation of information in the requisite regulatory reporting format. The goal is to reduce errors that may arise on account of multiple manual entries. This use of technology also has the added benefit that it can enable an audit trail for the reported information, which is particularly useful if a sanctions lookback needs to be conducted.

In addition to the above, many organisations apply "Robotics Automation" for the elimination of the excessive manual touchpoints in the sanctions review processes and information consolidation requirements. This can assist organisations in increasing operational efficiencies, reduce sanctions review timelines and applicable costs.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

Both the EU, via EU Commission guidance (see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN and https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.I.2018.277.01.0004.01.ENG&toc=OJ:C:2018:277I:TOC), and the German government, via BAFA (see http://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_icp_en.pdf?__blob=publicationFile&v=3), have recently become more vocal on how they expect individuals and companies under their jurisdiction to implement sanctions and export control laws and regulations.

In principle, while there is no obligation to maintain a compliance programme, the responsible persons must prove "the due care of a prudent manager faithfully complying with his

duties", see http://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_icp_en.pdf?__blob=publicationFile&v=3 (referring to section 93 of the German Stock Corporation Act), which will be – to say the least – facilitated by maintaining a risk-based compliance programme.

The guidance provided by the EU Commission and BAFA is similar and suggests that management, in the area of sanctions and export control, set up an internal export control programme, which should include the following components: a regularly repeated risk assessment; management commitment to the objectives of sanctions and export control compliance; an organisational structure and distribution of responsibilities reflecting the results of the risk assessment; sufficient human and technical resources and other (IT) work equipment to address the identified risks; appropriate process organisation; record-keeping and storage of documents; diligent staff selection, training and awareness raising, as well as regular reviews of process and system controls (ICP audits), taking appropriate corrective actions if the need may be; the establishment of a whistle-blower system; and assuring physical and technical security.

It is observed that leading organisations focus on specific risk factors such as geographic locations of business operations, risks posed by third parties, suppliers, and their intermediaries, along with the specific risks posed by product and services. Organisations are keen to put in place a comprehensive root cause analysis ("**RCSA**") framework, for the deficiencies identified in the control testing process.

Continuous review mechanisms around the recent global sanctions enforcement actions are also key to account for any policy related updates required. This may also assist how businesses prioritise their risk assessment programmes. One such business area, for instance, could include mergers and acquisitions, where businesses need to carry out more detailed due diligence exercises regards sanctions risk assessments of the primary and associated entities of the new business relationship.

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Yes.

Violations of EU Sanctions and German foreign trade law, including Germany's export control regime, may be punished as criminal offences or as administrative offences.

Intentional violations constitute criminal offences. According to section 17 para. 1 AWG, for example, a violation of an arms embargo constitutes a criminal offence and is punishable by imprisonment of up to 10 years. Furthermore, a fine may be imposed and determined according to the offender's individual financial situation/income and the offence.

Negligent violations of EU Sanctions and German foreign trade law, including Germany's export control regime, are generally considered administrative offences. "Negligence" is defined as not exercising the necessary standard of care ("*Fahrlässigkeit*"). As per section 19 para. 6 AWG, such administrative offence may result in a fine of up to EUR 500,000 per offence and forfeit of gains resulting from the administrative offence committed.

Further details can be found at http://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_icp_en.pdf?__blob=publicationFile&v=3.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

The authority responsible for investigating and prosecuting criminal Economic Sanctions is the public prosecutor's office at the court which exercises local jurisdiction over the breach of sanctions (section 143 para. 1 of the Courts Constitution Act ("**GVG**")).

The competent public prosecutor's office will be assisted by the competent authority administering the sanctions (in case of Financial Sanctions, the Bundesbank, and in case of Economic Sanctions, the BAFA); see question 1.2 above.

Only in rare and extremely exceptional cases may the Federal Prosecutor General take over the investigation (section 142a GVG); *e.g.*, if the sanctions violation investigated has the potential to disrupt or endanger national security or external security of the foreign relations of the Federal Republic of Germany.

4.3 Is there both corporate and personal criminal liability?

Yes.

While the concept of corporate criminal liability does not exist under German law, corporations still may face administrative penalties based on the Act on Regulatory Offences ("**OWiG**").

Specifically, under section 30 OWiG, the corporation may be fined if certain executive employees, specifically executive employees with the power to represent the corporation, have committed a criminal offence or a regulatory offence, *e.g.*, a breach of applicable sanctions laws and regulations, as a result of which duties incumbent on the corporation have been violated, or where the corporation has been enriched or was intended to be enriched.

Furthermore, under section 130 OWiG, if the owner or certain executive employees, specifically executive employees with the power to represent the corporation, intentionally or negligently omit to take the supervisory measures required to prevent contraventions, *e.g.*, breaches of applicable sanctions laws or regulations, such owner or executive employee may be held liable. An example of this would be the failure to implement an effective internal compliance programme resulting in a breach of sanctions laws or regulations by an employee whom the owner or the executive employee was supposed to supervise.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

In general, and if a maximum fine is not specified in the particular law, the maximum fine for individuals should not exceed EUR 1,000, section 17 para. 1 OWiG. However, section 19 para. 4 AWG punishes administrative offences of individuals in the context of sections 19 para. 1, para. 3 No. 1 lit. a, para. 4 sentence 1 No. 1 with a maximum fine of up to EUR 500,000. Other administrative offences regarding the AWG are to be punished with a maximum fine of up to EUR 30,000. The exact amount depends on the economic circumstances of the offender.

According to section 30 para. 1 OWiG, if the institution or a member of the institution authorised to represent a legal entity, the executive or a member of the board of directors of an association, a shareholder authorised to represent a legal entity or any other executive commits a criminal or administrative offence which violates the responsibilities of or enriches or was supposed

to enrich the legal entity, it – this means the legal entity itself – can be punished with an administrative penalty. In the case of an intentional criminal offence, a fine of up to EUR 10 million can be imposed; in the case of a negligent criminal offence, a fine of up to EUR 5 million can be imposed (section 30 para. 2 sentence 1 OWiG). If the violation in the context of section 30 para. 2 OWiG is an administrative offence, the maximum fine is governed by the particular violated law, section 30 para. 2 sentence 2 OWiG. If the particular law governing the administrative offence refers to section 30 para. 2 sentence 3 OWiG, the maximum fine multiplies by 10.

In any case, the maximum fine can be significantly higher if section 17 para. 4 sentence 1 OWiG is applicable. Section 17 para. 4 sentence 1 OWiG states that the fine is supposed to be higher than the economic advantage for the offender. According to section 17 para. 4 sentence 2 OWiG, every particular maximum fine can therefore be exceeded significantly if the economic advantage for the offender is higher than the maximum fine. Section 17 para.4 sentence 1 OWiG is also applicable regarding fines according to section 30 para. 1 OWiG, section 30 para. 3 OWiG.

4.5 Are there other potential consequences from a criminal law perspective?

Yes.

As further consequences of a violation of sections 17, 18, 19 AWG, objects to which the offence or administrative offence relates, and objects that were used or intended for their commission or preparation, may be confiscated pursuant to section 20 AWG.

In practice, a breach has practical consequences with regard to the customs authority. In response to a breach, the customs authority may suspend or revoke authorisations or customs simplifications that have been granted. The consequences particularly affect export-oriented companies. Finally, the audits carried out by a customs authority depend on the risk profile of the company. Thus, if the customs authority has noticed an increase in the number of infringements committed by the company in foreign trade and has already imposed fines, the frequency of the company's audit automatically increases.

As a further potential consequence, according to section 124 I No. 3 GWB, contractual authorities may exclude a company from participating in any award procedure if the company has committed serious misconduct while doing business questioning its integrity. As the awarding authority has scope for assessment when determining if a company has committed serious misconduct questioning its integrity, possibly a violation of sections 17, 18, or 19 AWG, this could lead to an exclusion according to section 124 para. 1 No. 3 GWB.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

Yes.

The AWG also provides for civil law consequences of a negligent violation against economically imposed sanctions. The requirements for a fine are found in section 19 para. 1 AWG in connection with 18 para. 1 AWG. Furthermore, as an example, the courts might find a termination void and, therefore, unenforceable in case such termination was itself a breach of the EU Blocking Statute. See question 2.11 above.

4.7 Which government authorities are responsible for investigating and enforcing civil Economic Sanctions violations?

The local public prosecutor's office and customs, with assistance of the Bundesbank and BAFA, are responsible. See question 1.2 above.

4.8 Is there both corporate and personal civil liability?

Yes, see question 4.3 above.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

According to section 19 para. 6 AWG and section 30 para. 2 OWiG, a fine may be imposed up to a maximum of EUR 500,000. It should be noted that section 17 para. 4 OWiG provides the possibility to impose fines higher than the maximum fines regulated by law in cases where the economic benefit which the offender received is greater than the maximum fine regulated by law ("*disgorgement*").

However, the maximum fine can be significantly higher if section 17 para. 4 No. 1 OWiG is applicable. Section 17 para. 4 No. 1 OWiG states that the fine is supposed to be higher than the economic advantage for the offender. According to section 17 para. 4 No. 2 OWiG, every particular maximum fine can therefore be exceeded significantly if the economic advantage for the offender is higher than the maximum fine. Section 17 para. 4 No. 1 OWiG is also applicable regarding fines according to section 30 para. 1 OWiG and section 30 para. 3 OWiG.

4.10 Are there other potential consequences from a civil law perspective?

Yes, see question 4.5 above.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

The public prosecutor's office and the German customs administration are in charge of investigating and enforcing administrative offences. The particular penalty is assessed by the (district) court.

The principle of individualised sentencing is regulated in section 46 of the German penal code ("*Strafgesetzbuch*") ("**StGB**"). This means that the assessment of penalties is especially based on the individual economic and personal circumstances of the convict, as well as the factual circumstances of the offence. The penalty, expressed in so-called "*Tagessätze*", which means a daily rate over a certain time is subdivided into the amount of the penalty per day and the number of days the convict needs to pay. This means that the particular penalty can be adjusted to the economic circumstances of the convict.

The imposition of fines is regulated in section 17 para. 3 OWiG. The assessment of fines is also based on the individual circumstances of the convict as well as the factual circumstances of the offence.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

In principle, the person or company concerned may appeal against the imposition of a fine. As a consequence, the public prosecutor may decide to grant the appellant's request. Otherwise, the matter is brought before the court.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

The public prosecutor's office, with assistance of the Bundesbank and BAFA, enforces sanctions on a national level; see questions 1.2 and 4.3 above.

Public prosecutor's offices on the level of the German federal states, with assistance from the Bundesbank and BAFA, enforce German national sanctions and export control law. There is no parallel state or local law applicable to sanctions and export control violations.

Only in rare and exceptional cases does the Federal Prosecutor General take over (section 142a GVG) the investigation. This only applies if the investigation reaches such a scale that its existence could disrupt or endanger national security or external security of the foreign relations of the Federal Republic of Germany.

4.14 What is the statute of limitations for Economic Sanctions violations?

The statute of limitations applicable is based on whether the sanctions violation is considered a crime or an administrative offence. Further, the statute of limitations applicable in cases where the sanctions violation is considered a crime depends on the maximum prison term associated with the specific sanctions violation.

In cases where the sanctions violation is a crime, specifically in cases of an intentional violation of an arms embargo, the limitation period is 10 years (section 17 para. 1 AWG, section 78 para. 3 No. 3 StGB). In certain offender-related circumstances (*e.g.*, gang membership), the limitation period is also 10 years (section 17 para. 3 AWG, section 78 para. 3 No. 3 StGB). For reckless violations of arms embargoes and intentional violations of EU Sanctions, the limitation period is five years (section 17 para. 4 AWG, section 78 para. 3 No. 4 StGB).

In cases where the sanctions violation is an administrative offence, *e.g.*, in cases of negligent breach of EU Sanctions, the limitation period is three years (section 19 AWG, section 31 para. 2 No. 1 OWiG).

5 General

5.1 If not outlined above, what additional Economic Sanctions–related measures are proposed or under consideration?

Further and additional EU Sanctions on Belarus are contemplated in light of the ongoing political situation in Belarus and specifically in light of the recent events in Japan concerning a member of the Belarus Olympic Team and the situation at the border of Lithuania.

5.2 Please provide information for how to obtain relevant Economic Sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

Official information regarding sanctions in non-EU states is published and frequently updated on a sanctions map provided by the EU Commission and can be accessed at: https://www.sanctionsmap.eu/#/main.

The above-mentioned EU law can also be found via the internet. See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FTXT and for the TEU see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012M%2FTXT.

German law is publicly accessible at https://www.gesetze-im-internet.de/titelsuche.html. A list of laws available in English can be accessed at https://www.gesetze-im-internet.de/Teilliste_translations.html (please be aware of the disclaimer under "*User-Notice*").

The leaflet published by the BAFA is very comprehensive and valuable to those new to this area of law as well as experienced practitioners. This nearly 20-sided document can be downloaded free of charge from https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Allgemeine_Einfuehrung/allgemeine_einfuehrung_node.html.

Further guidance for those new to the area of sanctions law can be found on the sanctions page of the European Union. Here, in a structure comparable to this article, individual questions regarding European sanctions law are answered; see https://eeas.europa.eu/headquarters/headquarters-homepage/423/sanctions-policy_en.

A basic overview of the institutions and the legislative process in the EU can be obtained at https://europa.eu/european-union/about-eu/institutions-bodies_de#rechtsetzung.

For comprehensive current developments and more detailed information, in particular, individual sanctions, see https://www.gibsondunn.com/2019-year-end-sanctions-update/; for detailed information on ICPs, see https://www.gibsondunn.com/new-guidance-on-internal-compliance-programs-what-regulators-on-both-sides-of-atlantic-expect-from-international-business/.

See https://www.gibsondunn.com/u-s-eu-and-un-sanctions-navigating-the-divide-for-international-business/ for a comprehensive overview of sanctions law, in particular a deeper insight into U.S. sanctions law is recommended: Adam Smith/Stephanie Connor/Richard Roeder, in *U.S., EU, and UN Sanctions: Navigating the Divide for International Business*, published by Bloomberg Law in 2019. Gibson Dunn's International Trade practice and the lawyers on our global sanctions team can help navigate the complex web of varying obligations and restrictions.

EY Forensic & Integrity Services can help companies with sanctions compliance and investigations along with remediation, see https://www.ey.com/en_gl/forensic-integrity-services.

Michael Walther is a partner in the Munich office of Gibson, Dunn & Crutcher LLP. His expertise has a multidisciplinary and international approach covering sanctions and export control, antitrust and competition, data protection and cybersecurity, as well as white-collar defence and investigations. He successfully advises German and international clients, many of which are active in technology-driven industries, on antitrust and competition law. He is regularly involved in complex transactions concerning acquisitions, joint venture scenarios and other forms of cooperation within the industry. He also regularly handles EU and German data privacy and cybersecurity matters.

Gibson, Dunn & Crutcher LLP
Hofgarten Palais, Marstallstrasse 11, 80539 Munich
Germany

Tel: +49 89 189 33 180
Email: mwalther@gibsondunn.com
URL: www.gibsondunn.com

Richard Roeder is a senior associate in the Munich office of Gibson, Dunn & Crutcher LLP. He focuses on international trade compliance and white-collar investigations, as well as transactional regulatory risk assessments, and advises clients from various industries in the areas of sanctions, anti-money-laundering and anti-corruption compliance. In 2018, Mr. Roeder was seconded to Gibson Dunn's Washington, D.C. office where he worked with the U.S. sanctions and export control team and specifically assisted clients in managing the challenges posed by the divergence between U.S. and EU economic and financial sanctions (e.g., regarding the EU Blocking Statute).

Gibson, Dunn & Crutcher LLP
Hofgarten Palais, Marstallstrasse 11, 80539 Munich
Germany

Tel: +49 89 189 33 115
Email: rroeder@gibsondunn.com
URL: www.gibsondunn.com

Meribeth Banaschik is a partner in EY's Forensics & Integrity Services team. As an American litigator and Solicitor of England & Wales with more than 15 years of professional experience, including 10 years' experience in Germany, Meribeth is focused on analytics and applied technologies to isolate and address various risks facing modern global organisations, particularly legal risks. She focuses on the measurement and quality imperatives that impact defensibility and acceptance of technology and technology-driven results in a legal/investigative context. In addition to leading the German eDiscovery and Managed Document Review practice, she is also responsible within Forensics for GDPR compliance projects, document intelligence and litigation operations.

EY Forensic & Integrity Services
Börsenplatz 1, Köln 50667
Germany

Tel: +49 160 939 14325
Email: meribeth.banaschik@de.ey.com
URL: www.ey.com

Bisman Sethi is a Director in EY's Forensic and Integrity Services team. As a Certified Fraud Examiner, with specialisation in Information Technology, Bisman focusses on evaluation and implementation of new technologies, with application of artificial intelligence (AI) in the field of AML and in Combating the Financing of Terrorism (CFT). She has assisted leading financial services organisations examine, assess and automate (using Intelligent Robotics Process Automation (RPA), their compliance processes for transformation and operational optimisation objectives. In addition, she also leads the Screening as a Service (SaaS) ecosystem and works back across the EU region in extending the API led, subscription services programme for sanctions, pep and adverse news for real time compliance monitoring requirements.

EY Forensic & Integrity Services
The Ruby, Dadar West, Mumbai
India

Tel: +91 9619001184
Email: bisman.sethi@in.ey.com
URL: www.ey.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: glg global legal group