McDermott Will & Emery

October 2018

McDermott International Legal Highlights

Table of Contents

Welcome to the second edition of the McDermott International Legal Highlights.

This publication includes a collection of articles, written by McDermott lawyers in the United States and internationally, focusing on recent and future legal challenges facing Japanese companies while expanding abroad. In this publication, we report on topics relevant to Japanese companies and on those which McDermott has strong capabilities and a developed skill set.

We hope that you find these legal news updates informative and engaging. Please feel free to contact your usual McDermott lawyer, or myself, if you have questions or points for clarification.

Jacques Buhart
Partner
Paris, Brussels
McDermott Will & Emery

How to Prepare for and Prevent Data Falsification Issues

Paul M. Thompson (Washington, DC)

In September 2015, news broke that Volkswagen had manipulated software on its diesel engine vehicles to avoid emissions requirements, a disclosure that led to the largest data falsification case in history. To date, the company has spent more than $34 billion in fines and settlements to deal with the crisis. In addition, a number of its senior executives have either pleaded guilty or been indicted in the United States.

But Volkswagen was just the start. For Japanese companies alone, there have been a rash of data falsification cases. Takata and Toyobo recently resolved such cases with the US Department of Justice (DOJ). Just last fall, Kobe Steel announced that it had falsified data to make it appear as though certain products met customer specifications, leading to lawsuits in the United States and Canada and a DOJ investigation. In December 2017, Keidanren asked its 1,500 members to investigate whether they had data falsification or quality control issues at their companies.

Since then, more than a dozen Japanese companies—including some of the country's largest—have publicly disclosed data falsification issues. In recent weeks, matters took a more serious turn when Tokyo prosecutors indicted Kobe Steel and three subsidiaries, as well as two former executives at Mitsubishi Materials, all for data falsification.

To be sure, data falsification is serious business. It is serious to US regulators and prosecutors, who have pursued civil fines and criminal prosecutions against international companies. And it is serious to Japanese prosecutors, who have already indicted two well-known Japanese companies and several former executives.

But the real question for counsel and compliance officers at Japanese companies is how to avoid these data falsification issues in the first place.

The answer lies in knowing the kinds of factors that give rise to data falsification issues in the first place. In recent cases, at least, there have been relatively consistent factors that pushed an otherwise well-meaning employee or company to engage in conduct that the US government and Japanese authorities would consider data falsification:

- Pressure to meet production deadlines
- Pressure to comply with demanding regulatory standards
- Pressure to respond to customer demands
- Lack of concern for minor testing errors that do not pose safety concerns
- Pressure to generate profit

While these pressures are understandable, there is only one way to ensure that compliance trumps them: establish and implement an effective compliance program. If your company does not have a compliance program that seeks to address the risks posed by data falsification, then you need one—and you need one right away.

The elements of an effective compliance program are set forth in the US Sentencing Guidelines and are well known. USSG § 8B2.1. They center on a few basic ideas: a company must "exercise diligence to detect and prevent criminal conduct," id. at § 8B2.1(a)(1), and it must "promote an organizational culture that encourages ethical conduct and compliance with the law," id. § 8B2.1(a)(2).

A review of data falsification matters over the past few years shows common mistakes that prevent companies from identifying issues before it is too late. To avoid these pitfalls, a compliance program should include the following measures:

- Policies and procedures. Companies often are missing written policies and procedures, particularly ones that deal with data falsification. A company should have consistent policies from plant to plant or laboratory to laboratory. These policies should be in addition to the general guidance that a company provides to all employees about conducting themselves in an ethical and honest way, no matter the circumstances or the pressure to do otherwise.
- Responsible compliance officer. Every company that performs testing to meet customer, industry or regulatory standards should have a chief compliance officer (CCO), and many do. A common mistake, however, comes when that CCO delegates review of product design or testing questions to more technical professionals, such as engineers, plant managers or lab technicians. There are problems with this approach. To begin with, it is the job of the CCO, with a direct report to the board of directors, to identify and remedy compliance issues. This role must be independent and accountable, in order to provide the CCO with the authority to remedy problems without having to worry about the demands or agendas of other supervisors. No matter how technical this function is, the CCO should not delegate it away. If the CCO needs to bring in an expert or work closely with others in the company to understand an issue, he or she must do so. But the CCO must be ultimately responsible for getting to the truth.
- Effective training. To help combat data falsification issues, the company must provide regular training to its employees, preferably in person. The training should deal with difficult issues that arise at the plant floor or in the laboratory, and should provide concrete instructions on how to deal with those issues or where to seek more guidance. How should the employee deal with non-conforming products? If a product fails testing, can it be retested? And what if a customer acknowledges that a product has not passed certain tests, but insists on receiving it anyway for a discounted price? These issues arise every day, and your company should be thinking about and addressing them during its regular employee training.

- Regular but random audits. The company should conduct regular, random audits that follow an audit plan and are done in a consistent way from plant to plant. Many companies conduct audits but announce them well ahead of time, or do not have a consistent audit program.
- Enforcement/reporting. Every company should have an easy, effective way to report misconduct, and a concrete protocol for investigating those reports. In some cases that have led to data falsification settlements, internal whistleblowers raised issues long before the government opened an investigation. Those internal complaints, however, were either missed or not thoroughly investigated.

Getting your compliance program in order does not need to be a herculean task. The best way to determine whether you have gaps is to conduct a brief compliance check-up by assessing the items listed above and determining what, if any, additional steps your company needs to take.

For Japanese companies that manufacture products that must meet certain regulatory, contractual or industry standards, data falsification remains a big deal. The misconduct is often hard to uncover, and one mistake in testing can be replicated thousands of times without detection. To prevent these problems, a company must make compliance a priority and look for the gaps in its current compliance program, with a particular view toward the kinds of issues that arise in these cases. Doing so may take some time and cost some money now. It is, however, the most effective way to prevent larger problems down the road.

The General Data Protection Regulation: Key Requirements and Compliance Steps for 2018

Mark E. Schreiber (Boston) and Ashley Winton (London)

The General Data Protection Regulation (GDPR) is the biggest story of 2018 in the field of global privacy and cybersecurity. McDermott has covered both the requirements and immediate impact of GDPR before, but its key points bear repeating.

The GDPR is enforceable in all EU Member States since May 25, 2018 and expand the territorial scope of EU data protection law. The new regulation introduces numerous changes that will affect businesses' data processing operations and the way it deals with suppliers, customers and employees. It expressly applies to organizations/entities established outside the European Union that offer paid or free goods or services to EU data subjects or monitor EU data subjects' behavior. This gives the GDPR global reach, requiring compliance from organizations around the world, notably in Japan.

These important changes require action, according the following steps.

STEP 1: Mapping EU Personal Data and Processes, and Determining the Legal Basis for Processing

Achieving compliance first requires organisations to determine what types of personal data they process. The GDPR applies to "any information relating to an identified or identifiable natural person." Even if the data being considered does not contain or comprise personal data, it will still be treated as personal data under the GDPR if it can be correlated with other data or databases that can identify an individual.

Personal data must be processed "lawfully", "fairly" and in a "transparent manner", and "must be collected for specified, explicit and legitimate purposes", which now need to be recorded as part of the new requirement of Accountability.

STEP 2: Updating Data Protection Notices and Consent Language

Privacy notices are likely to be longer and more detailed and must include information such as the purposes of the processing and its legal basis, the recipients or categories of recipients of the personal data, and the period for which the personal data will be stored, amongst other additions. Consent language also needs updating, and it is a good idea to keep an audit trail to balance the reversal of the burden of proof in the GDPR.

STEP 3: Accommodating the rights of Data Subjects

The GDPR introduces new, and strengthens existing, data subjects' rights, including the right to data portability and the right to be forgotten. Procedures or policies for dealing with these need to be put in place.

STEP 4: Implementing Accountability

Controllers must now maintain an accountability database that keeps a record of all data processing activities.

The GDPR requires controllers to conduct a privacy impact assessment prior to processing operations that are likely to result in a high risk to the rights and freedoms of individuals.

One of the GDPR's major accountability innovations concerns the obligation to consider whether or not a data protection officer (DPO) needs to be appointed to oversee and audit data processing operations.

STEP 5: Mitigating Data Protection and Privacy Risks in Customer Contract and the Supply Chain

One of the most significant changes in the GDPR is its imposition of statutory obligations on data processors.

In addition, supply and customer contracts need to be updated to include additional language prescribed by the GDPR, including additional obligations on processors and additional restrictions on the use of sub-processors.

With the direct statutory obligation on processors, the reversal of the burden of proof, the ease in which damages can be determined in the European Union, and the new rules permitting quasi class actions, there is the risk that data subjects may sue processors for service failures that affect their enjoyment of products or services that they obtain from the processor's customers.

Contracts between controllers and processors should be reviewed to ensure that they incorporate the additional provisions of the GDPR, and appropriately allocate risk and liability.

STEP 6: Complying with New Cybersecurity and Data Breach Notification Obligations

The GDPR introduces new cybersecurity and general data breach notification obligations. It requires a cybersecurity review to be undertaken, which brings into scope a wide range of activities, such as service levels for availability, business continuity, disaster recovery, and regular penetration and other tests.

In the event of a data breach, controllers must notify the competent supervisory authority within 72 hours if the rights and freedoms of individuals are at risk. The data controller must also inform the affected data subjects if the breach is likely to result in a high risk to their rights and freedoms.

The controller is required to document any data breaches in order to enable the supervisory authority to verify whether the organisations complied with its obligations.

Organisations should review their cyber security positioning now and make sure that they have a support framework in place in case of any data breaches. The Article 29 Working Party has published further guidance on this subject.

Cross-Border Data Transfer Rules

The GDPR does not fundamentally change the current cross-border data transfer rules under the Directive. Controllers continue to be bound by strict rules when exporting personal data from the European Union.

However, failure to comply with these rules or to have the appropriate compliance structure in place will result in a higher level of risk for the controllers and processors with potential administrative fines of up to €20 million, or 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

With one common method of legitimizing the international transfer of personal data—the European Commission's "Standard Contractual Clauses"—under review in the European Court of Justice, it is important to undertake a review to ensure that compliance steps are up to date.

Anticipating Sanctions, Enforcement and Liability

The GDPR endows supervisory authorities with significant corrective powers, such as the power to issue warnings and impose hefty fines.

Not-for-profit bodies, organisations or associations may now lodge complaints and bring legal actions on behalf of data subjects.

Dealing with Supervisory Bodies

As a general rule, each supervisory authority will be competent "for the performance of the tasks assigned to and the exercise of the powers conferred on it... on the territory of its own Member State." The GDPR introduces a one-stop-shop system with respect to the processing of personal data connected to multiple Member States.

The lead supervisory authority will be required to cooperate with the other relevant supervisory authorities in the decision-making process.

EU General Court Confirms Parental Liability for Non-Pure Financial Investors

Mai Muto (Brussels)

On July 12, 2018, by its judgment in Case T-419/14 The Goldman Sachs Group v. Commission, the General Court of the European Union entirely dismissed the appeal brought by the Goldman Sachs Group, Inc., against the European Commission's decision in Case AT. 39610 Power Cables fining Goldman Sachs more than EUR 37 million for its parental liability for an infringement of EU competition law by one of Goldman Sachs's former indirect subsidiaries.

Commission Decision

On April 2, 2014, the Commission imposed fines on suppliers of underground and submarine high-voltage power cables for their participation in a global market and customer sharing cartel. Prysmian Cavi e Sistemi Srl (PrysmianCS) took part in the cartel from February 18, 1999, until January 28, 2009. Goldman Sachs was an indirect parent of PrysmianCS from July 29, 2005, until the end of the infringement by PrysmianCS.

The Commission held Goldman Sachs jointly and severally liable with PrysmianCS on the basis that Goldman Sachs was presumed to have exercised decisive influence over PrysmianCS between July 29, 2005, and May 3, 2007, and actually exercised such influence over PrysmianCS between July 29, 2005, and January 28, 2009.

According to the established case law, where a parent company has a 100 percent shareholding in an infringing subsidiary, the parent company is able to exercise decisive influence over the conduct of the subsidiary, and there is a rebuttable presumption that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary. From July 29, 2005, to May 3, 2007 (leaving aside an initial 41 days), Goldman Sachs held a shareholding of between 84.4 percent and 91.1 percent in PrysmianCS, falling short of 100 percent. Nevertheless, the Commission applied this case law to Goldman Sachs because Goldman Sachs indirectly held 100 percent of the voting rights in PrysmianCS during this period.

The Commission also found that Goldman Sachs indeed exercised decisive influence over PrysmianCS before and after May 3, 2007, the date on which shares in PrysmianCS were offered to the public in an initial public offering, on the basis of objective factors related to the economic, organizational and legal links between Goldman Sachs and PrysmianCS.

General Court Judgment

Goldman Sachs appealed the Commission's decision and especially disputed the Commission's application of the presumption of exercise of decisive influence, as well as the findings regarding the rebuttal of the presumption and the actual exercise of decisive influence.

The General Court upheld the Commission's application of the presumption of exercise of decisive influence. The Court confirmed that where a parent company is able to exercise all the voting rights associated with its subsidiary's shares, that parent company is in a position to exercise total control over the conduct of that subsidiary without any third parties, even if it does not hold all or virtually all the share capital of the subsidiary. The Court then found that even after Goldman Sachs's divestments of equity in PrysmianCS, Goldman Sachs continued to be able to exercise 100 percent of its

voting rights because the divestments were subject to conditions ensuring that the new shareholders could not exercise any voting rights associated with their shareholding.

The Court also upheld the Commission's finding that Goldman Sachs failed to adduce sufficient evidence to rebut the presumption.

Further, the Court agreed with the Commission's conclusion that Goldman Sachs indeed exercised decisive influence over PrysmianCS during the entire period from July 29, 2005, until January 28, 2009, although it dismissed one of the objective factors on which the Commission based its conclusion.

With regard to Goldman Sachs's claim that no parental liability should be attributed to it because it was a pure financial investor, the Court reiterated the definition of "pure financial investor" according to relevant case law: "an investor who holds shares in a company in order to make a profit, but who refrains from any involvement in its management and in its control." The Court found that Goldman Sachs failed to demonstrate that it refrained from any involvement in the management and control of PrysmianCS.

The General Court dismissed all the other arguments made by Goldman Sachs and dismissed Goldman Sachs's appeal in its entirety.

Comment

The General Court accepted that parental liability is not applicable to pure financial investors. However, the Court made it clear that investment banks and private equity firms do not fall automatically under the category of pure financial investors just because they are investment professionals. They must refrain from any involvement in the management and control of the subsidiary to be considered pure financial investors.

In light of the difficulty involved in qualifying as a pure financial investor, investment professionals should implement risk mitigation measures, including stricter due diligence before the acquisition of portfolio companies, and the introduction and reinforcement of antitrust compliance programs at portfolio companies, rather than refraining from those measures that might make them look more like industrial owners.

Merger Control in China Following the Termination of Qualcomm/NXP

Joel R. Grosberg (Washington, DC), Andrea L. Hamilton (Brussels), and Alex An (Shanghai)

What Happened

On July 26, 2018, Qualcomm announced the termination of its approximately US$40 billion acquisition of NXP following its inability to obtain SAMR's approval prior to the end date of July 25, 2018, resulting in Qualcomm being obliged to pay NXP US$2 billion as termination compensation. Although SAMR did not prohibit the transaction, its failure to approve the transaction effectively blocked it. It appears to mark the first time that China's antitrust regulators have not approved a global transaction that was approved by other global regulators—and, at least potentially, on non-competition grounds. Indeed, the US Federal Trade Commission gave its green light to Qualcomm/NXP without a second request, and the European Commission issued a conditional clearance early on January 18, 2018.

The fact that SAMR did not approve Qualcomm/NXP prior to the longstop date came as a surprise to many. Since China instituted the Antimonopoly Law in 2008, China has generally followed the lead of other major antitrust regulators, particularly the European Union. Where the EU and US antitrust regulators have imposed remedies, China has often imposed similar remedies, or in some cases imposed remedies designed specifically for the Chinese market. SAMR's failure to approve prior to the longstop date thus appears to mark a departure from the typical convergence—at least at a high level—in merger outcomes that has been prevalent over the past 10 years.

Questions have thus arisen as to whether SAMR's decision not to approve was due to legitimate antitrust issues or should be seen in the context of the current trade tensions between the United States and China. In a statement issued on July 27, 2018, SAMR indicated that the remedies proposed by Qualcomm had yet to address SAMR's competition concerns, and expressed regret that the parties had terminated the deal. Although SAMR's statement suggests that its actions were based solely on antitrust concerns, it appears plausible that geopolitical tensions between the United States and China contributed to the outcome. Notably, the Ministry of Commerce (MOFCOM), the predecessor to SAMR, had recently approved transactions in the semiconductor industry,

in some cases conditioned upon remedies similar to those accepted by other global antitrust regulators. The questions, therefore, are: what made the Qualcomm/NXP deal different, and was antitrust solely to blame or were other issues at play?

The acquisition of NXP by Qualcomm reportedly led to competition concerns relating to Qualcomm's baseband chipsets, NXP's NFC and SE chips, MIFARE technology and NFC technology. These concerns appeared to be resolvable through remedies, and public reports suggested that Qualcomm may have been close to resolving the issues during the course of SAMR's antitrust review. However, after the Trump administration threatened to impose significant tariffs on Chinese products in early July 2018, SAMR's review of Qualcomm/NXP appeared to encounter difficulties, which ultimately were unresolved. Indeed, almost two years after Qualcomm's agreement with NXP was signed, it is questionable whether Qualcomm would have been able to negotiate a remedy with SAMR in the current environment, even if the parties had decided to further extend the termination date. This may suggest that politics were a factor.

What This Means

The possibility that SAMR's effective "block" of Qualcomm/NXP could be—at least in part—politically motivated has given rise to general concerns about China's antitrust review of mergers in the current political environment, particularly those involving US companies.

While politics may have played a part in SAMR's actions vis-à-vis Qualcomm/NXP, this case is likely an outlier. Qualcomm/NXP was a high-profile transaction involving a sensitive industry (semiconductors), a major US company and some legitimate antitrust issues, and was thus a good candidate to use in retaliation for the tariffs imposed by the Trump administration. The measure may have been particularly symbolic given the importance the Trump administration has placed on Qualcomm and its 5G technology. Only recently, the Trump administration used the US Committee on Foreign Investment in the United States process to block Broadcom's attempt to take board control over Qualcomm partly because of concerns that Broadcom would not invest in or develop 5G like Qualcomm. As a result, Qualcomm was a strong candidate to send a message to the Trump administration concerning current trade tensions. Moreover, the fact that SAMR (and before it, MOFCOM) has granted antitrust approval to several transactions involving US firms lends support to the view that any political influence that was brought to bear in Qualcomm/NXP is an exception, rather than a "new normal."

Although the political situation remains fluid, at present it appears likely that only high-profile transactions involving US firms that have legitimate antitrust issues in sensitive industries are likely to be affected by the political tensions between the United States and China. Parties to such transactions may experience longer delays in obtaining antitrust approval, and possibly higher degrees of risk. Parties to such transactions can take steps to reduce potential risks, including for example the following:

- Set a flexible termination date. It is highly likely that the transaction may not be approved before the expiration of the longest review period, i.e., 180 days. The parties should bear in mind that the review period could be further extended by means of withdrawal and refiling in practice. Introducing flexibility can help accommodate lengthened reviews and provide sufficient time to negotiate remedies.
- Provide a reasonable termination fee in the event that SAMR fails to act.
- Be flexible with remedies. It is not uncommon for the China antitrust review authority to require further commitments specific to the China market. Introducing flexibility into what the parties consider to be reasonable remedies can also help accommodate the wider ranging requirements they may face in the current political environment.
- Maintain clear and frequent communication with the concerned authorities that have a say in the deal, not limited to SAMR.
- Companies should also stay attuned to developments affecting the trade dispute, as the political environment may become less predictable if the trade dispute escalates. Conversely, in the event that the trade dispute is resolved, the risks described in this article may dissipate.

Companies should also stay attuned to developments affecting the trade dispute, as the political environment may become less predictable if the trade dispute escalates. Conversely, in the event that the trade dispute is resolved, the risks described in this article may dissipate.

En Banc Federal Circuit: § 145 Appellants Do Not Have to Pay (Attorneys' Fees) to Play

Margaret M. Duncan (Chicago) and David Mlaver (Washington, DC)

The en banc US Court of Appeals for the Federal Circuit held that a dissatisfied patent applicant that chooses to appeal from a decision of the Patent Trial and Appeal Board rejecting claims of a patent application can appeal to the US District Court of the Eastern District of Virginia without fear of being required to pay the prorated salaries of US Patent and Trademark Office (PTO) employees who work on the appeal, regardless of the outcome. NantKwest, Inc. v. Iancu, Case No. 2016-1794 (Fed. Cir. July 27, 2018) (en banc) (Stoll, J, joined by Newman, Lourie, Moore, O'Malley, Wallach and Taranto, JJ) (Prost, CJ, dissenting, joined by Dyk, Reyna and Hughes, JJ).

NantKwest filed a complaint against the director of the PTO in the Eastern District of Virginia pursuant to 35 USC § 145, appealing from the PTO's rejection of its patent claims. After the district court affirmed the PTO's decision, the PTO filed a motion for reimbursement of "[a]ll the expenses of the proceedings," including its attorneys' fees in the form of the prorated salaries of the PTO personnel who worked on the appeal. Section 145 states that "[a]ll the expenses of the proceedings shall be paid by the applicant." The district court denied the PTO's motion for attorneys' fees because the American Rule provides that each party should pay its own attorneys' fees. The PTO appealed the denial, and a divided Federal Circuit panel reversed the district court. The Federal Circuit panel held that § 145 was a deviation from the American Rule and attorneys' fees were included in "[a]ll the expenses of the proceedings" (IP Update, Vol. 20, No. 7). The Federal Circuit next issued a *sua sponte* order to hear the appeal en banc and vacated the panel decision.

Under § 141, dissatisfied applicants may appeal directly to the Federal Circuit, the most routinely used path for appeal. But applicants also may use § 145 and seek review in the Eastern District of Virginia through the filing of a civil action. In such an action, the parties can conduct discovery and introduce new evidence, including oral evidence that was not presented to the PTO during prosecution. These § 145 actions are resolved under the same methods as traditional district court proceedings, such as motion practice and a trial on the merits. Unlike § 141 appeals, in § 145 proceedings, the applicant must pay "[a]ll the expenses of the proceedings." Ever since the predecessor statute of § 145 was passed in the mid-1800s, these expenses have included travel, expert and court reporter fees, and document production costs—but never attorneys' fees.

The en banc Federal Circuit ruled that the American Rule applies and the language of § 145 is not specific and explicit enough to be interpreted as including attorneys' fees. The en banc Court held that "the American Rule prohibits courts from shifting attorneys' fees from one party to another absent a 'specific and explicit' directive from Congress. The phrase '[a]ll the expenses of the proceedings' falls short of this stringent standard."

Practice Note: This case may be heading to the Supreme Court of the United States because the decision in NantKwest creates a split between the Fourth Circuit and the Federal Circuit in the interpretation of similar statutes (15 USC § 1071 (b) and 35 USC § 145) as to whether the American Rule applies and what is included in "all the expenses of the proceeding(s)" for appeals to a district court. Compare Shammas v. Focarino, 784 F.3d 219, 223–24 (4th Cir. 2015) with the NantKwest decision.

McDERMOTT INTERNATIONAL HIGHLIGHTS

7th McDermott International Seminar in Japan

Please join us for McDermott Will & Emery's 7th International Seminar in Tokyo, Japan. We hope to see you on January 29-30 to kick off of our two-day seminar delving into recent legal issues that are relevant to Japanese companies going abroad.

AUTHORS

For more information, please contact your regular McDermott lawyer, or:

Jacques Buhart
+33 1 81 69 15 01
jbuhart@mwe.com

Alex An
+86 21 6105 0595
aan@mwechinalaw.com

Margaret M. Duncan
+1 312 984 6476
mduncan@mwe.com

Joel R. Grosberg
+1 202 756 8207
jgrosberg@mwe.com

Andrea L. Hamilton
+32 2 282 35 15
ahamilton@mwe.com

David Mlaver
+1 202 756 8822
dmlaver@mwe.com

Mai Muto
+32 2 282 35 24
mmuto@mwe.com

Mark E. Schreiber
+1 617 535 3982
mschreiber@mwe.com

Paul M. Thompson
+1 202 756 8032
pthompson@mwe.com

Ashley Winton
+44 20 7577 6939
awinton@mwe.com

For more information about McDermott Will & Emery visit www.mwe.com