



SUPPLY CHAIN COMPLIANCE

WEEKLY NEWS AND COMPLIANCE STRATEGIES ON A GLOBAL LEVEL

Contents

- 1 Société Générale to pay USD 1.3 billion in penalty fees to US bodies
- 1 Report reveals worrisome numbers regarding human rights abuses in the supply chain
- 3 The GDPR: Rights of the individual
- 5 Blockchain as a supply chain risk mitigator
- 6 News Briefs

Société Générale to pay USD 1.3 billion in penalty fees to US bodies

French bank Société Générale S.A. agreed to a settlement with U.S. agencies regarding apparent violations of multiple sanctions programs, including the Cuban Assets Control Regulations (1963), the Iranian Transactions and Sanctions Regulations (2018), and the Sudanese Sanctions Regulations (2017). Between 2003 and 2013, the bank facilitated transactions worth more than USD 13 billion for entities in the aforementioned countries.

Under the terms of the settlement (<http://bit.ly/2zosmfR>), Société Générale agreed to pay a fine of USD 1.3 billion total to several agencies, and to enter into deferred prosecution agreements and consent decrees with those agencies for at least 18 months and as long as three years. If the bank does not violate any more sanctions regulations, the deferred prosecution agreements and consent decrees expire.

The bank will pay USD 53.9 million to the Office of Foreign Assets Control of the U.S. Department of the Treasury (OFAC), USD 717.2 million to the U.S. Attorney's Office of the Southern District of New York, USD 162.8 million to the New York County District Attorney's Office, USD 81.3 million to the U.S. Federal Reserve, and USD 325 million to the New York State Department of Financial Services. "This amount is entirely covered by the provision for disputes booked in Société Générale's accounts," representatives of

continued on page 4

Report reveals worrisome numbers regarding human rights abuses in the supply chain

The Corporate Human Rights Benchmark (CHRB) released its 2018 key findings for the apparel, agricultural products and extractive industries in early November. The U.K.-based organization draws on publically available data from governments, think-tanks, investors and business foundations to determine how companies perform across 100 indicators, based primarily on the U.N.'s Guiding Principles on Business and Human Rights (<http://bit.ly/2DDf1Dx>). The report focused on six major themes: Governance and policy commitments, embedding respect and human rights due diligence, remedies and grievance mechanisms, performance of a company's human rights practices, performance of a company's responses to serious allegations, and transparency. It found that the majority of companies scored very low across the board, with only a few companies showing true dedication to embedding human rights into their risk assessments and due diligence procedures.

"The overall picture is deeply concerning; most companies score poorly on the Benchmark, indicating weak implementation of the U.N. Guiding Principles on Business and Human Rights," wrote Steve Waygood, chief responsible investment officer at Aviva Investors and chair of the CHRB. "This raises questions for investors and consumers as to

continued on page 2



Managing Editor

Margaret Martyr
margaret.martyr@
corporatecompliance.org

Reporter

Sascha Matuszak
sascha.matuszak@
corporatecompliance.org

Proofreader

Patricia Mees
patricia.mees@
corporatecompliance.org

Design & Layout

Pete Swanson
pete.swanson@
corporatecompliance.org

whether these companies are serious about avoiding harm to people in their pursuit of profits.”

More than two-thirds of companies tracked by the report scored less than 30 percent overall, and a quarter of companies scored less than 10 percent. Higher scoring companies, including Rio Tinto Group and Adidas AG, were outliers, but they demonstrated that fast improvement is possible. “There were alarmingly low scores in some areas of systemic challenge which serves to highlight how far business has to go,” added Phil Bloomer, member of the advisory council at CHRB. “The alignment of purchasing practices with human rights is not easy, but without this, in food and apparel, abuse in their complex global supply chains is inevitable.”

One of the biggest challenges for companies, according to the findings, is responding properly to serious allegations and ensuring lasting remedies: “Over a third of the serious allegations reviewed were not publicly responded to and less than half of the allegations of serious negative human rights impacts resulted in meaningful engagement with alleged affected parties. Further, of the almost 100 allegations reviewed, only 3 percent of cases show to provide remedy that was satisfactory to the victims.”

Report on Supply Chain Compliance (RSCC)

(ISSN: 2637-7543) is published 45 times a year by the Society of Corporate Compliance and Ethics, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435, USA. +1 952.933.4977, www.corporatecompliance.org.

Copyright © 2018 by the The Society of Corporate Compliance and Ethics (SCCE). All rights reserved. On an occasional basis, it is okay to copy, fax or email an article from RSCC. Unless you have SCCE's permission, it violates federal law to make copies of, fax or email an entire issue; share your subscriber password; or post newsletter content on any website or network. To obtain permission to transmit, make copies or post stories from RSCC at no charge, please contact customer service at +1 952.933.4977 or service@corporatecompliance.org. Contact Kari Henderson at +1 952.405.7927 or kari.henderson@corporatecompliance.org if you'd like to review our very reasonable rates for bulk or site licenses that will permit weekly redistributions of entire issues.

Report on Supply Chain Compliance (RSCC) is published with the understanding that the publisher is not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

Subscriptions to RSCC include free electronic delivery in addition to the print copy, as well as a searchable database of RSCC content and archives of past issues at www.corporatecompliance.org.

Human rights in the supply chain

For supply chain managers and compliance officers, the key measurement theme is “Performance: Company Human Rights Practices.” This theme covers topics critical to ensuring supply chain integrity and compliance with accepted norms and standards, such as:

- » Ensuring a living wage.
- » Mapping and disclosing the supply chain.
- » Eliminating forced and child labor.
- » Health and safety.
- » Freedom of association.
- » Women’s rights.
- » Working hours.

Companies tracked by the report generally scored very poorly in this measurement theme, with the average score being 20 percent. For example, at least 90 percent of companies were unable to show that they pay living wages, provide company guidelines for contractual arrangements, and share details of how they work with suppliers to improve living wages in their supply chains.

In regards to child labor, forced labor and indebted bondage, companies in general scored very low. Only four companies scored full points regarding child labor, meaning that they were able to disclose how they deal with child labor when it is identified, and how they work to transition children from work to education. More than 90 percent of apparel companies and more than 60 percent of agricultural products companies were unable to show how they protect workers from paying fees or other costs (including the forced surrender of personal identification) before being allowed to work. Companies performed just as poorly in terms of protecting women’s rights, tenant and community land rights, and working hours.

Companies generally scored best on health and safety, especially the extractive industry. Nearly a third of extractive companies gained full points in this topic by disclosing quantitative information on health and safety (e.g., injury rates and fatality rates) for both their direct employees and seasonal and migrant workforce. They also provided explanations of their figures, their set targets related to rates of injury and whether these targets were met; additional background information was also given on the targets that weren’t met.

Takeaways

- » A report on how corporations protect human rights within the supply chain shows the majority do not pay enough attention to those issues, focusing instead on profit and increasing shareholder value.
- » Companies that scored well on the report’s benchmark are also among the most successful businesses in the world, demonstrating that attention to human rights has a positive effect on profits and shareholder value. 

The GDPR: Rights of the individual

Ireland's Data Protection Commission (DPC) is arguably the most important of the European Union's commissions enforcing the GDPR. Several major tech companies have their European headquarters in Ireland, making the DPC the first line of regulatory enforcement for tech giants such as Google LLC, Facebook, Inc., Paypal Holdings, Inc., Microsoft Corp., eBay Inc. and LinkedIn.

The DPC runs two separate sites, one legacy site (<http://bit.ly/2qYh7Gg>) from before the GDPR came into effect, and the new site (<http://bit.ly/2DQX1X2>) that is currently under construction. Both sites have important information and guidance for individuals and organizations subject to the GDPR. One of the more important pieces of information (<http://bit.ly/2TvI8hn>) deals with the rights of individuals under the GDPR, of which there are eight major rights:

1. Right to be informed.
2. Right to access information.
3. Right to rectification.
4. Right to erasure.
5. Right to data portability.
6. Right to object to processing of personal data.
7. Right of restriction.
8. Rights in relation to automated decision making (profiling).

These rights are not only critical for individuals to understand but also for organizations that control or process the personal data of EU citizens around the world.

Know your rights: The first four

The "right to be informed" (Articles 13 and 14 of the GDPR) is the first and most important right under the GDPR. This right stipulates that the data controller (i.e., the "person, company, or other body which determines the purposes and means of processing of personal data") must provide a trove of information to individuals whose personal data is being collected. Along with contact details for the data controller and data protection officer within the controller's organization, some of the required information includes:

- » Purpose(s) of the processing and the lawful basis for the processing.
- » Where applicable, details of any intended transfers to a third country (non-EU member state) or international organization and details of adequacy decisions and safeguards.
- » The retention period (how long an organization holds onto data).
- » The existence of any automated decision making processes that will be applied to the data, including profiling, and meaningful information about how decisions are made, the significance and the consequences of processing.

The controller is bound to provide this information within a reasonable amount of time, but access to the information must be requested (i.e., the "right to access" [Article 15]). When it is requested, the data controller is bound by law to promptly provide the information in a transparent, concise and easily accessible format, electronically if so requested. The DPC has instructions (<http://bit.ly/2PHELFT>) for making a request for information, or requesting access to any personal data processed and collected by the controller.

The "right to rectification" and the "right to erasure" (also known as the "right to be forgotten") allow individuals or organizations to require data controllers to rectify inaccurate data, or have personal data erased under certain circumstances:

- » Where personal data is no longer necessary in relation to the purpose for which it was collected or processed.
- » Where the individual withdraws his/her consent to the processing, and there is no other lawful basis for processing the data.
- » Where the individual objects to the processing, and there is no overriding legitimate grounds for continuing the processing.
- » Where the individual objects to the processing, and his/her personal data is being processed for direct marketing purposes.
- » Where personal data has been unlawfully processed.
- » Where personal data have to be erased in order to comply with a legal obligation.
- » Where personal data has been collected in relation to the offer of information society services to a child.

There are also circumstances in which the right to be forgotten does not apply:

- » Exercising the right of freedom of expression and information.
- » Compliance with a legal obligation, the performance of a task carried out in the public interest or in the exercise of official authority.
- » Reasons of public interest in the area of public health (See Article 9(2)(h) & (i) and Article 9(3), GDPR).
- » Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- » Establishment, exercise or defense of legal claims.

Know your rights: The last four

The "right to data portability" (Article 20) refers to the ability to "obtain your personal data from a data controller in a format that makes it easier to reuse your information in another context, and to transmit this data to another data controller of your choosing without hindrance."

Individuals also have the "right to object to processing of personal data" (Article 21). This right allows individuals to contact a data controller and state the grounds upon which they object to the collection and processing of the data. This right is strong when the processing relates to direct marketing, but it is somewhat weaker when the

processing relates to “tasks in the public interest, or under official authority, or in the legitimate interests of others.”

The “right of restriction” (Article 18) enables individuals to restrict processing actions of data, such as deletion, for four specific reasons:

- » Objecting under Article 21.
- » Contesting the accuracy of the data.
- » Concluding the processing was unlawful.
- » Requiring the data for the purpose of a legal claim.

Individuals can also object to their personal data being processed by automated means, under the “rights in relation to automated decision making (profiling)” (Article 22). Automated processing is only permitted with an individual’s express consent, when necessary to perform a contract or when authorized by EU or Member State law. The automated processing of the special categories of personal data is only lawful after the person has given express consent and where the processing is necessary for reasons of substantial public interest.

Takeaways

- » The individual rights enshrined in the GDPR represent the strongest pro-consumer data privacy regulations in the world.
- » Consumers must know and exercise their rights under the GDPR in order for the regulation to have the intended effect. ▽

Société Générale to pay USD 1.3 billion

continued from p. 1

the bank wrote in a statement (<http://bit.ly/2Tzwkld>). “These agreements will not have an additional impact on the Bank’s results for 2018.”

According to a statement (<http://bit.ly/2zoQ4Zk>) released by the U.S. Attorney’s Office for the Southern District of New York, Société Générale “operated 21 credit facilities that provided significant money flow to Cuban banks, entities controlled by Cuba, and Cuban and foreign corporations for business conducted in Cuba ... The majority of these transactions and most of the total value involved a U.S. dollar credit facility designed to finance oil transactions between a Dutch commodities trading firm and a Cuban corporation with a state monopoly on the production and refining of crude oil in Cuba.”

The statement also details communications between the bank’s compliance department and senior management regarding transactions with Cuba, OFAC and potential penalties for violations: “[W]e have lived with the OFAC list for some time and have developed various methods of avoiding it,” a senior leader of group compliance allegedly wrote, “given the new regulatory scrutiny in the U.S. on USD payments do we remain satisfied with those methods?”

Mitigation and compliance

Although the penalty of USD 1.3 billion counts as the second largest levied for sanctions violations to date, the amount was reduced considerably due to the bank’s cooperation with the investigation and other mitigating factors. In a press release, Société Générale itself listed the many changes it has made to its compliance department to help prevent similar violations in the future.

In its enforcement information released Nov. 19, OFAC listed the mitigating factors:

- » Société Générale S.A. has not received a Penalty Notice or Finding of Violation from OFAC in the five years preceding the date of the earliest transaction giving rise to the Apparent Violations.
- » Société Générale S.A. cooperated with OFAC’s investigation of the Apparent Violations by conducting an internal investigation, responding to multiple requests for information in a timely manner, and executing a statute of limitations tolling agreement with multiple extensions.

The bank also took the following remedial actions:

1. Terminated the conduct outlined above and has established, and agrees to maintain, policies and procedures that prohibit, and are designed to minimize the risk of the recurrence of, similar conduct in the future.
2. Created a centralized sanctions compliance function, implemented key enhancements at the group level, and implemented enhancements within the business lines that were subject to the review.
3. Increased the number of personnel within compliance staffing, and [Société Générale’s] total budget for sanctions compliance has also increased.
4. Implemented a more comprehensive training regime for employees across the group and various business lines, including a group-wide general training program. Group Sanctions Compliance has also developed targeted, in-person training for employees with a higher risk of exposure to sanctions-related transactions.

“These specific actions supplement important measures that the Bank has already taken regarding the organization and operation of its compliance program,” the bank declared in a statement. “Notably, they include a vast multi-year compliance transformation program, the implementation of a centralized and independent compliance role directly supervised by General Management, and the deployment of a worldwide “Culture & Conduct” program.

“We aim to meet the highest standards of compliance and ethics in the best interest of our clients and of all of our stakeholders,” added CEO Frédéric Oudéa.

Takeaways

- » Société Générale’s recent sanctions violations and money-laundering and bribery actions result in record

finances, including the second largest penalty for a sanctions violation.

- » The French bank has committed itself to sweeping changes within its compliance department to ensure that any further problems are found, fixed, and prevented. 

Blockchain as a supply chain risk mitigator

Industries from shipping to agribusiness to energy hail the digitalization of a wide variety of procedures and operations as a critical part of the fourth industrial revolution (<https://on.wsj.com/2AatO5i>) and a panacea to many supply chain ills. One of the key technologies being introduced into supply chain management is blockchain, a decentralized digital ledger that allows multiple parties to communicate and share authenticated data without the need for an intermediary organization.

Supply chains often suffer from inconsistent or unavailable data, a lack of interoperability between scattered stakeholders, and incomplete information on a product's lifecycle or transport history. A shipping company, for example, may have to deal with multiple paper copies of a traditional bill of lading that are distributed to the various parties involved in shipping goods from one place to another, such as the carrier, the overseas consignee and the destination port. If a copy goes missing or is altered, the process to replace it can cause significant delays. Blockchain is essentially the digitization of the entire process, but instead of various traditional systems (e.g. information technology) latching on to each other as best as possible, firms can look to a single chain of "blocks" containing all relevant data (*RSCC, 6-July-2018, p. 5*).

There are countless blockchain projects and initiatives currently underway. Several of the more promising ones deal with supply chain issues.

Shipping pilots

Two major blockchain initiatives that arose in the last year focus specifically on the shipping industry. The first, announced Aug. 9 (<https://ibm.co/2R3KbYf>), is a collaboration between A.P. Moller–Maersk Group and IBM Corp., called TradeLens (<http://bit.ly/2Q8S55L>).

The pilot program involves more than 90 participants, including more than 20 port and terminal operators, customs authorities from multiple countries such as The Netherlands and Peru, several freight forwarders and logistics companies, and major global container carriers Pacific International Lines and Hamburg Süd Group. According to a press release, using the TradeLens blockchain ledger could "reduce the steps taken to answer basic operational questions such as 'where is my container' from 10 steps and five people to ... one step and one person." A presentation put together by TradeLens partners (<http://bit.ly/2qVSIbI>)

describes in great detail the burdens that the global shipping industry faces (e.g., inefficient paper-based processes) and the ways in which blockchain ledger eliminates much of that burden. According to the presentation, the partners expect full commercialization of the pilot by the end of 2018.

The second pilot, the Global Shipping Business Network (GSBN), was announced Oct. 24 at China International Import Expo's Blockchain Supply Chain Forum (<http://bit.ly/2RMMa3k>) and involves nine ocean carriers and terminal operators, including carriers CMA CGM S.A. and COSCO SHIPPING Ports Ltd., and terminal operators DP World and Hutchison Ports Holdings Ltd. The group is working together with CargoSmart Ltd. and represents a challenge to the IBM-Maersk led consortium.

These are just two of the more well-known blockchain pilots. The Port of Rotterdam, for example, is also seeking to digitalize its processes (<http://bit.ly/2AxWI66>) with help from the Samsung Group and ABN AMRO Bank N.V.

Roar Ådland, visiting scholar at the MIT Center for Transportation & Logistics, writes in the Supply Chain @ MIT blog that these two competing blockchain solutions threaten to fragment an industry, and that fragmentation defeats the entire purpose of a blockchain ledger. He suggests a supranational solution to avoid silos and isolation: "But to reach its full potential, perhaps the development of [shipping blockchain platforms] needs to be a supranational — not a purely commercial — effort at this critical stage. Maybe a U.N. trade body is better placed to steer the emergence of blockchain-enabled technology in shipping? The involvement of such an organization would be at a global level, so as not to stifle private sector innovation."

Farm to fork

The concept of farm-to-table is now firmly embedded in the social consciousness and, coupled with costly recalls, is driving big food producers to seize control of their supply chains in order to ensure the type of quality consumers are increasingly demanding.

Walmart Inc. recently signed on with the IBM Food Trust (<https://ibm.co/2zCC5zD>), a "collaborative network of growers, processors, wholesalers, distributors, manufacturers, retailers and others enhancing visibility and accountability in each step of the food supply," through the use of IBM's blockchain platform. The retailer then mandated that direct suppliers of several different food items join its blockchain by Jan. 31, 2019, and that farmers, logistics firms and business partners of these suppliers join the blockchain by Sept. 30, 2019.

The move to a blockchain ledger comes at a time when food quality and security is a major issue for consumers. Walmart faced an eruption of E. coli linked to romaine lettuce early this year. As investigators worked to trace the contamination, 210 people got sick and five died, according to the U.S. Centers for Disease Control and Prevention.

Takeaways

- » Major corporations across a variety of industries are investing in blockchain technology to bring efficiency and transparency to complex supply chains. The technology is officially mainstream.
- » The process of implementing blockchain technology across a global value chain requires input and effort from all stakeholders. The investment in time, capital, and human resources is huge, but the payoff can be equally significant. \

NEWS BRIEFS

◆ **US grants waiver for Chabahar Port.** A port in southern Iran that services Afghanistan and India (*RSCC, 16-Nov.-2018, p. 1*) has been exempted from U.S. sanctions against Iran. The port is a geopolitical asset for the U.S. in that it gives India access to landlocked Afghanistan at the expense of Pakistan. The U.S. hopes that Indian influence on Afghanistan can further U.S. national security goals. “This exception relates to reconstruction assistance and economic development for Afghanistan. These activities are vital for the ongoing support of Afghanistan’s growth and humanitarian relief,” a U.S. Department of State spokesperson said in a statement.

The Maritime Executive reports that the “new Indian-run port at Chabahar will also serve to counterbalance China’s regional influence. China’s government recently financed a competing port project just across the border in Pakistan, where it is investing up to USD 60 billion in a giant network of transportation and energy infrastructure, the China Pakistan Economic Corridor.”

The Maritime Executive: <http://bit.ly/2DPaHSI>

◆ **China to tighten cybersecurity and tracking regulations.** The Cyberspace Administration of China issued new rules this week requiring online service providers to keep extensive records of user information, including real names, log-in and log-off times, network source addresses and types of hardware used. All of this data will be shared with the government. Service providers are also required to police their platforms and report any speech or behavior that may contradict or go against government laws and regulations. The move affects all domestic service providers; it’s unclear how foreign companies, such as Google LLC, would be affected by the new regulations.

The regulations codify existing practices, and they may be reminders to online service providers that the Chinese government is serious about policing the internet. Next year, two major anniversaries commemorating uprisings against the government are taking place: the 100th anniversary of the May Fourth Movement and the 30th anniversary of the Tiananmen Massacre. It’s likely that the Chinese government is preparing for those anniversaries with crackdowns online that also coincide with strong crackdowns on university free speech and freedom of association.

The Financial Times: <https://on.ft.com/2KvgP2V>

Axios: <http://bit.ly/2Qiba5C>

◆ **Turkeys now traceable back to farm.** Major turkey processors Jennie-O Turkey Store and Cargill, Inc. have implemented traceability programs that allow consumers to learn more about the sources of their turkeys. Jennie-O’s program uses labels that contain codes that can be entered on the Jennie-O website, where consumers will be taken to an informational page that details the region where the turkey was raised, pictures of the farm owners and a quote from the farmer.

Cargill’s program utilizes blockchain technology to trace their Honeysuckle White brand of turkeys back to their sources. A Cargill press release from October 2017 describes the advantages of blockchain technology in the supply chain: “Blockchain models build a trusted, transparent food chain that integrate key stakeholders into the supply chain and create a distributed ledger with immutable records. Because all participants inside the blockchain network must agree before a new record is added to a ledger, the technology also reduces the risk of fraud or human error, and cryptography within the network ensures security, authentication and integrity of transactions.”

Cargill press release: <http://bit.ly/2DQHIDe>

The Star Tribune: <http://srib.mn/2qXqNAZ>

◆ **Presidents Donald Trump and Xi Jinping to meet at G20 summit.** After a year of tense negotiations and rising trade conflicts, the leaders of China and the U.S. will meet on the sidelines of the G20 summit in Buenos Aires, Argentina to discuss concessions and possible solutions to the trade war. The U.S. and China have imposed tariffs on billions of U.S. dollars of goods in the past year, leading to disruptions in global supply chains, plummeting fortunes for certain industries, including American agriculture and Chinese steel, and the loss of opportunities for other players to enter the market, such as Southeast Asian and European suppliers. The trade war is set to escalate at the beginning of 2019, when the U.S. will raise tariffs from 10 percent to 25 percent on more than 200 goods imported from China.

The U.S. side presented the Chinese government with a list of 142 demands, and China responded with a list of concessions that did not meet many of the demands and did not include any major new offers to fend off the impasse between the two countries. Any talks would only set up a “framework” and would most likely not affect U.S. plans to raise tariffs in January 2019.

Bloomberg: <https://bloom.bg/2KpGhqi>