JONES DAY | One Firm Worldwide℠

WHITE PAPER

November 2018

Companies in France Need a Global and Consistent Culture to Face Unprecedented Regulatory Scrutiny

France's Sapin II Law, the nation's first regulation requiring companies of a certain size to implement anticorruption programs, has introduced a compliance culture that far surpasses corruption-related matters.

Beyond the implementation of an anticorruption program, companies doing business in France need to create and implement compliance programs and related internal procedures in a growing number of regulatory areas in order to meet regulatory requirements and to protect their reputation. In light of the multiplication of areas where compliance programs are needed, companies should establish a global and coordinated approach, taking their cue from the framework set by the Sapin II Law.

This Jones Day *White Paper* provides an overview of each of the various areas that may apply to your particular company and that should be included in a global and consistent compliance approach.

TABLE OF CONTENTS

INTRODUCTION

In an era of unprecedented increase in regulatory constraints on economic actors, it is crucial for companies to identify applicable regulations, resulting actions to be implemented, and internal compliance and control processes to set up. The Sapin II Law, the first French regulation making it a requirement for companies of a certain size to implement an anticorruption compliance program, has triggered a new and topical compliance culture that far exceeds the corruption-related matters.

Depending on your company's business, compliance programs should notably be established in accordance with the Sapin II Law, and meet the newly required, and heightened, duty of care (i.e., the "duty of vigilance") in the areas of corporate social responsibility, General Data Protection Regulation ("GDPR"), disclosure of ultimate beneficial owner, EU and U.S. sanction and embargo policies, trade secret protection and competition law. Health care companies are also required to comply with the Sunshine Act and anti-gift regulations and there are specific compliance and controls programs that must be implemented by financial institutions.

An overview of each of the following regulatory hot topics, highlighting the key points to have in mind and the main recommended actions for companies, is set forth in this document.

- The new French regulation relating to transparency, fight against corruption, and modernization of economic life set forth in the so-called "Sapin II law";
- The duty of care (*devoir de vigilance*) arising from a French law dated March 27, 2017;
- The European GDPR;
- The EU and U.S. sanction/embargo policies in connection with companies' day-to-day business as well as in connection with M&A transactions and investments;
- The EU Directive on the protection of Trade Secrets of June 8, 2016, and its implementation in EU countries including France on July 30, 2018.
- The new obligation for companies and branches located in France to disclose their ultimate beneficial owner, integrated in French law by an ordinance dated December 1, 2016, and applicable since August 1, 2017;
- The environmental, health, and safety regulations;
- Compliance with competition law;
- The Sunshine Act; and
- The compliance, controls, and anti-money laundering ("AML") obligations over financial institutions;

OVERVIEW: SAPIN II LAW DATED DECEMBER 9, 2016

Since June 1, 2017, French companies of a certain size are due to set up a corporate compliance program, internal alert systems, and a reporting procedure for whistleblowers that must comply with complex and dense regulations. These requirements are among other measures aimed at promoting transparency and fighting against corruption.

KEY POINTS	RECOMMENDED ACTIONS
Targeted Persons: Presidents, senior executives (*directeurs généraux*), managing directors (*gérants*), and *Société Anonyme* board of directors members of companies that (i) employ at least 500 employees or are part of a group with at least 500 employees with a parent company headquartered in France, and (ii) have an annual revenue or consolidated annual revenue exceeding €100 million. When the company issues consolidated accounts, the obligations lie on the company, as well as its subsidiaries and the companies it controls. The company is also liable if it fails to fulfill the obligation to implement a compliance program as required. ***Note*:** Setup of reporting procedure for whistleblower concerns companies employing at least 50 employees (see below).	Assess whether the French anticorruption Sapin II Law applies to your company, its French subsidiaries, and the latter's subsidiaries following the guidelines on the scope of the Sapin II Law's compliance program obligations issued by the newly created French Anticorruption Agency ("AFA").
Targeted persons must set up a corporate compliance program including: • A **corporate code of conduct** defining and illustrating conduct to be avoided that constitutes corruption or influence-trafficking offenses. Such code should be appended to the company's internal rules and subject to the procedure of information and consultation of employee representatives, in accordance with article L. 1321-4 of the French Labor Code; • An **internal alert system** to collect reports emanating from the company's employees reporting on the existence of conduct or situations violating the company's code of conduct; • A **regularly updated risk map** in the form of documentation intended to identify, analyze, and prioritize the company's risk exposure to external corrupt solicitations, notably regarding the business sector and geographic area in which the company pursues its activities; • **Integrity review** of clients, "first-tier" suppliers, and intermediaries in light of the risk map; • **Internal or external accounting controls** to ensure that the company's records are not covering up corruption or influence-trafficking offenses; • **Training for employees and managers** who are the most exposed to risks of corruption and influence trafficking; • A **sanction policy**, including disciplinary action against personnel found to have engaged in misconduct; and • **Internal controls and evaluation** of the measures implemented. Reporting Procedure for whistleblowers must be set up by entities employing at least 50 employees. According to a government decree dated April 19, 2017, this procedure should be implemented since January 1, 2018. Entities shall make a simplified declaration to the French National Commission for Data Protection and Liberties ("CNIL") if they implement an automated processing of personal data (see CNIL deliberation n°2017-191 dated June 22, 2017).	• Audit your company's or group's compliance program in light of the Sapin II Law (including interviews of employees). • Identify the provisions to implement and the steps to take in order to update your compliance program, in accordance with the recommendations of the AFA published on December 22, 2017 **and other subsequent guidelines**. • Update your compliance program. • Include the new corporate code of conduct in the company's regulations. • Set up procedures of treatments of breaches of the internal code. • Train your teams. • Liaise with the AFA.

OVERVIEW: DUTY OF CARE (*DEVOIR DE VIGILANCE*) ARISING FROM FRENCH LAW, DATED MARCH 27, 2017

Large French companies must set up internal care plans (which are rendered public) in order to mitigate or anticipate breaches of corporate social responsibility ("CSR") rules, including by their subsidiaries, suppliers, and subcontractors. The set up, and moreover the implementation of such plans, vis-à-vis suppliers and subcontractors, may turn out to be difficult in practice.

KEY POINTS	RECOMMENDED ACTIONS
Targeted Persons: Companies employing (directly or via their subsidiaries) at least 5,000 employees in France or 10,000 employees worldwide. **Scope:** Covered CSR matters include human rights and fundamental freedoms, health and safety of persons and to the environment.	Assess whether this regulation applies to your company.
Targeted persons are **liable for a "duty of care" (*devoir de vigilance*)** with respect to CSR matters including within their suppliers' and subcontractors' activities. **Targeted persons must implement an internal care plan containing:** • Risk mapping; • A periodic evaluation process with respect to the subsidiaries, suppliers, and subcontractors; • Proposed actions to mitigate risks or anticipate any significant breach of CSR rules; • An internal alert system to collect testimony of such breaches; and • An internal process for monitoring the above measures. The care plan, as well as an annual reporting of its implementation, must be provided in the annual management report of the concerned company and, as a consequence, is public. Any third person with legitimate interest (*justifiant d'un intérêt à agir*) can act before French Courts and request that the company receives an injunction, along with a financial penalty, to comply with their obligations to establish and update an internal care plan. Such an action is governed by ordinary French civil law. Indemnification of third parties may not be excluded if the claimant evidences the existence of a breach of the duty of care (*devoir de vigilance*) obligation, although the provisions providing for indemnification in the Law of March 27, 2018, have been cancelled by the French Constitutional Court.	• Audit your company's or group's activity, as well as your suppliers' and subcontractors', in order to identify CSR relevant matters. • All stakeholders concerned by your company's or group's business (i.e., all the persons who are involved in CSR matters and also in your activity) must be involved in the elaboration of the care plan. • Since the content of the care plan is not clearly defined in the law, it is worth referring to other tools with respect to CSR policies already in place within your company, such as ISO standards. • Coordinate with, and implement these new measures in consideration of, the other applicable regulatory constraints such as those arising from Sapin II law, which also provide similar prevention and care undertakings. • Train your teams, in particular with respect to monitoring and reporting matters that are permanent obligations. • Make sure that the plan is updated on a regular basis.

OVERVIEW: GENERAL DATA PROTECTION REGULATION

Published in 2016, the GDPR is a major revision of the legal framework applicable to the processing of personal data. It applies in all EU Member States as of May 25, 2018, and significantly increases the penalties for noncompliance with the data protection regulations.

KEY POINTS	RECOMMENDED ACTIONS
The GDPR reinforces and harmonizes the former existing legal framework for the processing of personal data. **Scope:** GDPR (i) applies to all businesses and individuals processing personal data, and also to their subcontractors; (ii) applies to the processing of personal data by entities established in the EU but also by entities located outside of the EU if the processing of data relates to the supply of goods or services to individuals located in the EU, or relates to the monitoring of the behavior of individuals within the EU. Breaches may be sanctioned by administrative fines of up to the greater of €20 million or four percent of the worldwide turnover of the undertaking.	Assess whether your company processes personal data, and if so, whether such processing activity relates to the EU and is subject to the GDPR.
• **Reinforcement of certain existing rights of the data subjects** (stronger requirements for consent, broader obligation of information). • **Creation of new rights in favor of the data subjects:** right to erasure of personal data, right to portability, right to restrict the processing of personal data. • Obligation to **set up internal processes** in order to protect personal data from their initial collection and processing; assessment of the data protection impact of processing activities entailing high risks for the privacy of data subjects. • Mandatory **appointment of a data protection officer** in certain situations. • **Data protection procedures** must be set forth in internal policies. • **A record of data processing activities** must be established and maintained. • **The GDPR creates direct obligations for subcontractors for the protection of personal data and the documentation of data processing activities.** Agreements with subcontractors must be amended to provide additional specific protections of personal data (confidentiality, no sub-subcontracting without prior consent, etc.). • **Obligation to disclose any personal data breach** to the relevant supervisory authority and to the concerned person in certain cases. • **Prohibition of international transfers of personal data** to countries outside of the EU not providing sufficient protection, unless appropriate safeguards are implemented.	• Inventory of the existing processing activities involving personal data; and assessment of the legal basis upon which your company relies for such activities (particularly when the consent of individuals is required). • Update of the information notices provided to the data subjects. • Implementation of procedures in order to comply with the new right to erasure and right to portability of personal data. • Creation of internal policies in order to ensure compliance with the principles of privacy by design and privacy by default. • Preparation of new documentation required: record of processing activities, data protection assessment for high risk data processing activities. • Assessment of the necessity to appoint a data protection officer. • Review of agreements with subcontractors and assessment of whether they need to be amended. • Evaluation of the technical and organizational measures applied to secure the data processing. • Define and implement a notification and response procedure to prepare data breaches. • Mapping of international data transfer flows and verification that such transfers comply with the specific applicable requirements.

OVERVIEW: EU AND U.S. SANCTION/EMBARGO POLICIES

Economic sanctions and export control regulations require careful attention, including through the implementation of policies and procedures to ensure compliance and avoid potentially severe civil and criminal fines and liabilities. In addition, in the context of any acquisition or investment, both buyers and sellers are advised to review the compliance situation in this area carefully and upstream.

KEY POINTS	RECOMMENDED ACTIONS
• **Key jurisdictions throughout the world have enacted significant economic sanction programs:** – The European Union currently has sanction programs in effect for more than 20 countries (as well as additional noncountry specific programs); – The United States also has sanction programs in effect that target more than 20 countries (as well as other non-country specific programs); and – Other key jurisdictions (including Australia, Canada, Japan, and others) have implemented sanction that may be relevant to multinational businesses. • **These sanction programs prohibit or restrict (depending on the program):** – Any direct or indirect dealings with designated individuals and entities; and – Specific activities such as imports and exports of certain goods, technology, and services (sometimes in certain sectors such as oil and gas), providing financing or insurance, and even indirect involvement in dealings with targeted countries and persons. • Violations can give rise to civil and criminal liability, result in the breach of financing and similar covenants, and/or close off or reduce future financing opportunities.	• Review and analyze business activity against relevant EU, U.S., and other sanction laws and regulations, as well as all application export control rules. • Identify all relevant points of risk for the business. • Review and assess company sanction and export control policies and procedures to ensure that they address the company's risks. • Implement a sanction and export control policy to mitigate compliance risks and reduce the risk of inadvertent violations.
• It is possible to conduct certain activities in sensitive countries, subject to complying with all applicable regulations. • Companies are increasingly knowledgeable concerning their obligations in this area. However, the rules can be very technical and require careful analysis to ensure compliance, especially in terms of permitted activities. • Acquiring a company or a business with activities in sensitive countries involves risk, both for the seller and the buyer, in respect of past, unremediated violations and future compliance. It is possible to address this risk through due diligence and contractual provisions.	• Tailor the policy to the objectives and risk profile of the company to mitigate risk. • Include relevant contractual provisions in agreements with third parties to protect the company. • Implement training for key personnel and management, and plan for periodic updates. • In the context of corporate transactions/M&A: – Buyers should conduct appropriate risk-based due diligence early in the transaction to determine if there are any issues, and include appropriate representations, warranties, covenants, and indemnities. – Sellers should consider reviewing the compliance situation of any business to be sold before engaging in any sale process to prevent surprises, and ensure that any issues are identified, resolved, or minimized.

OVERVIEW: TRADE SECRET PROTECTION

Know-how and information represent an important part of many businesses' intellectual capital, as they provide a competitive advantage and are a determining factor of competitiveness and innovation-related performance on the market. The Directive (EU) of 8 June 2016 and the national implementing laws have harmonized and strengthened the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure. Such protection is available only if the trade secret has been subject to "reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret." This condition requires more than just the intention to protect the trade secret, and calls for active and organized measures of protection. Finally, proper know-how management should not only be focused on a company's own information, but should also take into account received information, as a lack of control thereof (through poorly drafted non-disclosure agreements or unsolicited reception of information) can create risk of "contamination," preventing further search or file patents in a given field.

KEY POINTS	RECOMMENDED ACTIONS
Targeted Persons: Any business and noncommercial research institution, irrespective of their size, working in an environment in which know-how and information provide a competitive advantage, in particular businesses relying heavily on technical or commercial innovation.	• Make sure that appropriate trade secret management policies, procedures, and processes are implemented throughout the company or the group. • Ensure proper implementation of internal procedures and processes.
• **In the absence of appropriate trade secret policies and procedures:** – The company may simply be unable to rely on trade secrets to protect its intellectual assets; it needs to be able to prove that "reasonable steps have been taken under the circumstances, by the person lawfully in control of the information, to keep it secret"; – The company is more exposed to dishonest practices aimed at misappropriating its trade secrets; and – The company is exposed to "contamination" of its activities by third parties' trade secrets and thus to litigation. • **Audit existing trade secret protection policies and procedures.** – Audit existing internal policies, procedures and processes; – Audit clauses in all relevant contracts: ○ Clauses in employment contracts to ensure confidentiality and regarding ownership on trade secrets; ○ relations with suppliers or subcontractors; ○ standard NDA; ○ additional remuneration for employee-inventors; and – Determine the most important trade secrets and take immediate steps to protect them.	• Set up classes of data and information according to their importance and sensitivity for the company and define rules of access (preferably based on a need-to-know system). • Set up policies and procedures to identify and protect internal trade secrets: – Identification of trade secrets (different types and origin of trade secrets); – Manage declaration of trade secrets by employees; – Record, date, and gather evidence of trade secrets; – Control access to information within the company and within the group; – Compartmentalize the information; and – Regular updates. • Management of received trade secrets: – Monitor and prevent unsolicited reception of information; – NDA: drafting, signature, and recording; and – Prevent contamination. • Ensure control of confidential information through: – Physical access control; and – Electronic document management. • Set up internal procedures and process for the most frequent situations: – Set standard clauses for the most relevant contracts; – Manage signing and recording of such contracts; – Monitor arrival and departure of employee holding trade secrets; – React in case of identified violation of trade secret (theft, unauthorized copying, economic espionage, or breach of confidentiality requirements); and – Control scientific publication and other communication. • Train employees in the protection of trade secrets, appoint gatekeepers, and ensure proper implementation.

OVERVIEW: DISCLOSURE OF ULTIMATE BENEFICIAL OWNER

Since August 1, 2017, French companies and entities are required to disclose to a special registry the identity of the individual(s) who ultimately control(s) them and keep this information updated. This new regulation may, in certain cases, entail difficult situations for the French managers.

KEY POINTS	RECOMMENDED ACTIONS
Targeted Persons: Unlisted French companies, French economic interest groups, foreign companies having a registered branch in France, other legal entities having legal personality and registered in France. In case of breach, criminal sanctions may apply: • **Against the legal representative (individual) of the targeted person:** a six-month period of imprisonment and a fine of €7,500; additional sanctions may be decided, such as the prohibition of managing companies; and • **Against the targeted person (legal entity):** a fine of €37,500; additional sanctions may be decided such as the prohibition to submit to public procurements.	Identify each of the French companies, French branches, or other French economic group of your group to which the French UBO declaration obligation applies.
Targeted persons must **collect and keep comprehensive and up-to-date information** with respect to their ultimate beneficial owner(s) ("UBO"). They must **disclose details of**, and certain information with respect to, their UBO (name, nationality, personal address, date upon which he/she became a UBO, etc.) to the registry of the Commercial Court: • Within 15 days of deposit of their incorporation file for entities created since August 1, 2017; or • Before April 1, 2018 for entities incorporated prior to August 1, 2017. Updates of this UBO declaration must be made at the Commercial Court upon occurrence of any event (increase of share capital, transfer of shares, other, whether at the level of the targeted person or within its group above) triggering a change of UBO, and within 30 days as from such event. With respect to targeted persons being companies, the UBO is defined as being the individual who holds, directly or indirectly, more than 25 percent of the share capital *or* voting rights of the targeted person, or exercises, by any mean, the power to control the managing bodies or the shareholders' meeting of the targeted person. If information on the UBO cannot be collected, then, by default, the legal representative of the targeted person will be designated as being the UBO. The UBO declaration is filed at the registry of the Commercial Court, but it is not a public document. It is accessible to certain French authorities, such as judicial authorities, customs, tax administration, anticorruption authorities, in certain cases under certain conditions. In addition, any person who evidences being legitimate to access to the UBO declaration, may request the French judge to authorize such communication to him or her. French judge may request, by injunction, the defaulting targeted person to proceed to such UBO declaration. French judge may also appoint a specific attorney to do so; the latter is then entitled to request the auditor of the targeted person to communicate to him or her all necessary information he or she may have.	• Audit your company's or group's chain of control to identify the UBO of existing entities. • Set up internal processes and policies within your group in order to ensure that the legal representative of the targeted person is informed in due time of any change of the UBO further to the occurrence of any event within the group, or above the parent companies. • Set up cross borders European exchange on this topic within your group (UBO disclosure arising from a European directive applicable to all Member States since June 26, 2017). • Inform and train your teams. The detailed definition of the UBO and the criterion to assess the control of the targeted persons are somehow still unclear in the current applicable French texts. An application decree (*décret d'application*) has been announced and should clarify these aspects but is still missing. The clerk of the Commercial Court of Paris has proposed a template for the UBO declaration, which, within a pragmatic approach, should be used and complied with. The targeted person and its legal representative must keep evidence of the internal processes and actions implemented in order to collect the information required on the UBO, in particular if, at the end, they do not succeed in obtaining them.

OVERVIEW: ENVIRONMENTAL, HEALTH, AND SAFETY COMPLIANCE

The scope of environmental, health, and safety ("EHS") regulations in Europe and, in particular, in France is very wide and constantly evolving. Such regulations provide for various operating requirements, permitting and reporting obligations. They are also the basis for investigations by public authorities and often trigger liabilities related to EHS issues, which should be anticipated.

KEY POINTS	RECOMMENDED ACTIONS
EHS issues are key in a number of activities, including the **operation of industrial facilities**; **the use, storage, or transport of chemical and/or hazardous products or waste**; **the manufacturing, use, or selling of products** (including consumer and pharmaceutical products)**; real estate transactions**; etc. **EHS regulations are increasingly stringent and constantly evolving** pursuant to European and national regulations.	• Identify the EHS requirements related to your activities. • Keep up-to-date with EHS new regulations, obligations, and standards. • Anticipate regulatory investigations. • Identify and mitigate potential EHS liabilities.
• **Legal and technical EHS audits include:** - Operational permit review/compliance with operational requirements; - Buildings permits; - Asbestos in buildings; - Emission assessments (air, water, ground, and underground); - Present/past exposure of employees to hazardous substances including asbestos; - Assessment of sanitary risks; - Assessment of historical pollution and related costs; - Analysis of site operational history; - Baseline reports (required by regulations or for the purpose of a deal); - EHS financial guarantee assessments/verification; and - Product audit (eco-design requirements, health & safety issues). • It is crucial to **review technical EHS audits from a legal standpoint** to identify potential liability issues, report requirements to the official authorities, and negotiate contractual provisions. • EHS compliance audits may help to **identify potential EHS regulation violations, propose corrective actions, and limit liabilities** (criminal, administrative, indemnities to third parties).	• **It is required by law to undertake EHS compliance audits in a number of circumstances:** - Request from the environmental authorities; - Baseline report; - Partial or total termination of industrial activities; and - Identification of product noncompliance and/or health issues. • **It is strongly recommended to perform an EHS audit in certain situations:** - Share or asset deal (vendor or acquirer due diligence); - Sales of real estate property; - Prior to signing a lease; - Change in regulatory requirements; and - Assessment of your company/group's operational compliance with EHS regulations on a regular basis. • Conduct a pre-acquisition or pre-divesture EHS audit (with legal and technical coverage). • Negotiate environmental provisions in share or asset deals, or in leases. • Prepare mandatory and/or voluntary EHS disclosures in order to anticipate and mitigate corrective actions.

OVERVIEW: COMPLIANCE WITH COMPETITION LAW

The French Competition Authority and the European Commission regularly open new investigations of suspected infringements of competition law. The increasing use of leniency, settlement, and commitments procedures has significantly lightened their burden. At the same time, the fines imposed have continuously increased to reach millions or, in some cases, billions of euros. Now more than ever, companies must be prepared and have a robust, tailor-made compliance program in place. In its "Framework document on antitrust compliance programs," the French Competition authority insists that "there is no 'one size fits all programme.'"

KEY POINTS	RECOMMENDED ACTIONS
Targeted Persons: Competition law applies to "undertakings," i.e., to any entity engaged in an economic activity (regardless of its corporate form or how it is financed). Corporate groups are considered as forming one single undertaking. Consequently, fines are calculated at the group level. **Consequences:** A fine of up to 10 percent of the turnover achieved by the undertaking in the most recent fiscal year; damages in civil actions; imprisonment for fraudulently playing a personal and significant role in designing, organizing, or implementing the infringement; and reputational damage.	Make sure that a seamless compliance program is implemented throughout the undertaking (parent company and undertakings, in France and abroad).
The French Competition Authority has highlighted five key features of an efficient compliance program. 1. **Top management commitment.** 2. **Set up a compliance function** clearly identified throughout the organization, with adequate powers and resources to ensure effective implementation of the compliance program and direct access to senior management. 3. **Identify existing or past competition law issues.** This will allow the organization to put an end to the infringement if it is ongoing, but also to determine whether it wishes to report the issue to the relevant competition authority(ies) and benefit from the leniency procedure. 4. **Information and specifically-tailored training of all employees**, with a particular emphasis on those most exposed (senior management, pricing and marketing teams, anyone attending trade organization meetings or trade shows). 5. **Ensure continued compliance by having a process in place for employees to seek advice and confidentially report potential issues.** Whistleblowing systems must comply with data privacy requirements. Set proportionate and effective disciplinary sanctions in case of violation of the organization's compliance policy.	• Issue an official board statement on compliance commitment. • Review high-risk activities (any exchanges with competitors, trade association activities, refusal to supply, termination of distributors and agents, etc.) with in-house counsel. • Carry out a risk assessment to identify the areas in which the organization is most exposed. • Perform a document review of the main corporate documents and commercial agreements. • Interviews employees. • Organize training sessions and/or set-up web-based training tools. • Make periodic training a requirement for the most exposed employees. • Keep a record of who has been trained and when the training took place. • Issue competition law compliance guidelines. • Have employees sign a commitment to comply with the competition law compliance guidelines. • Test the various components of your compliance program (e.g., mock dawn raids). • Carry out internal audits, especially at critical times such as when acquiring a new business.

OVERVIEW: THE SUNSHINE ACT AND ANTI-GIFT REGULATIONS (HEALTH CARE COMPANIES)

Health care companies that manufacture, and/or market health products in France are subject to specific requirements regarding their relationships with health care professionals. This regime include anti-gift regulations (applicable since 1993) and disclosure requirements regarding conventions and benefits provided to health care professionals ("Sunshine Act," applicable since 2012).

KEY POINTS	RECOMMENDED ACTIONS
The French anti-gift regulations prohibit health care companies that manufacture and/or market health products that may be reimbursed by the French Social Security scheme from providing any benefit to health care professionals. Exceptions include: • Medical/scientific research; and • Hospitality granted to a health care professional during a medical/scientific event. In order to be granted an exception, the competent professional board must have prior review of the contract with the health care professional. Criminal and administrative penalties apply in case of noncompliance.	• Assess whether your health care company manufactures or markets health products that may be reimbursed by the French Social Security scheme. • Set up/update a company policy regarding relationship with French health care professionals. • Anticipate contract review by the professional board when applicable.
Pursuant to the French Sunshine Act, health care companies must disclose (i) the existence of convention, (ii) remunerations, and (iii) benefits provided to health care professionals. Broad scope of the Sunshine regulations: • Health care companies include all companies manufacturing or placing on the French market a wide range of health care products (including drugs, medical devices, cosmetics, etc.) and include international companies; and • Health care professionals include medical personnel but also medical associations, health establishments, etc. Disclosed information is made public on an official website held by the French Health Ministry. Criminal and administrative penalties apply in case of noncompliance.	• Assess your health care company's obligations with respect to Sunshine obligations. • Set up/update a company policy regarding relationship with French health care professionals. • Organize the collection of information to be disclosed.

OVERVIEW: COMPLIANCE AND CONTROLS IN FINANCIAL INSTITUTIONS

Financial institutions are heavy regulated entities that have to comply with detailed rules about their organization, the processes to be implemented, and their efficiency and the necessity to trace any action taken in this area. These rules include a set of principles aimed at ensuring their overall compliance with any law applicable to them, as well as their robustness to the various types of risks generated by their banking or financial activities. Compliance with anti-money laundering ("AML") rules applicable to each transaction offered to a client, which are subject to specific European legislation, is of particular importance. Investigations by supervisors (*Autorité de contrôle prudentiel et de résolution* or *Autorité des marchés financiers*) are regularly carried out against financial institutions and should be anticipated. In this particular area, it is left to the institutions to demonstrate their compliance (and not to the supervisors to do so), which make it crucial to have proper operational procedures that are effectively applied to any activity of the institution.

KEY POINTS	RECOMMENDED ACTIONS
Targeted Persons: Credit institutions, investment firms, asset managers, financial advisors, payment service providers, electronic money issuers.	• Ensure proper implementation of internal procedures and processes, complying with relevant rules and regulations. • Keep up-to-date with these regulations, obligations, and standards. • Anticipate regulatory investigations.
• **Compliance Functions:** Set up a compliance function with proper, and if necessary, dedicated resources that: – Covers general compliance of the carrying out of each type of activities with applicable laws and regulations (French, European, or international); – Monitors conflicts of interest; – Monitors confidentiality issues and inside information; – Ensures consistent application of procedures across the whole group (including in foreign branches or subsidiaries); and – Shall be independent from a hierarchy perspective, from all business lines. • **Control Functions:** Set up a dual line of controls (first and second level) in addition to an audit function that: – Properly cover all the risks identified and mapped by the risk function; – Has sufficient resources that are independent, from a hierarchy perspective, from all business lines; – Precisely report all controls conducted, and if applicable, detail all remediation plans to be implemented; and – Implement tools that are properly tailored to the actual risks faced by the institution with accurate control indicators. • **AML Functions:** Set up an AML function dedicated to the fight against money laundering and terrorism financing that is: – Based on an exhaustive analysis of AML risks generated by the business carried out, the products or services offered, the types of customers, and the way these products or services are proposed to these customers; and – Defines the proper processes of monitoring the onboarding of new clients and transactions entered into by them.	• Inventory of the activities that involve (i) the mapping of the services that are provided; (ii) the status, place of residence of customers; and (iii) the type of products and the level of risk embedded into them. • Procedures and policies precisely tailored to the actual organization of the company and the way the business is carried out. • Frequent controls of (i) the proper implementation of the procedures; (ii) remediation plans; and (iii) any situation that has shown a weakness in the organization or procedure. • Keep procedures and processes up-to-date with new rules or regulations, or new activities, products, or clients. • Regularly inform and train your teams dedicated to compliance control and AML functions. • Monitor all your activities abroad to ensure proper compliance abroad with French rules and regulations. • Have a proper policy in place in case the financial authorities conduct an investigation, including the designation of a single individual as point of contact and a policy for disclosing or transmitting any information to such authorities.

PARIS COMPLIANCE TEAM AT A GLANCE

Jones Day in Paris has created a team of lawyers with a deep knowledge and understanding of all the areas of compliance who are working seamlessly to help clients develop a tailored coordinated and consolidated compliance approach.

Our clients benefit from our experience through the implementation and review of global, custom-made compliance programs. We know that every one of our compliance-related practices has a role to play in this respect and their combined knowledge is our most valuable asset.

Jones Day's clients' needs and demands urged the Paris compliance team to envision a global coordination of all the companies' obligations and good practices in all matters impacted by compliance. Although each compliance field has its specificities, we believe that each practice may improve and enhance its approach and processes with the experience in other areas and, therefore, cross-practice efforts make our Paris compliance team a powerful one.

The Paris compliance team's global approach is eased by its multidisciplinary nature, since our team includes members from the following practices:

- Antitrust & Competition Law;
- Capital Markets;
- Cybersecurity Privacy and Data Protection;
- Environmental, Health & Safety;
- Financial Institutions Litigation & Regulation Law;
- Intellectual Property;
- Investigations & White Collar Defense;
- Labor & Employment;
- Mergers & Acquisitions; and
- Other practices as need be.

Details of the main contacts of the team are included at the end of this document.

The team assists clients with sanction issues and the implementation of compliance policies under French, U.S., UK, and other jurisdictional laws.

Focus Areas

- Internal investigations on sanctions, anticorruption, IT issues, and cybercrime.
- Assistance in "dawn raid" type situations or financial investigations.
- Extensive experience in the area of product safety, including regulatory compliance analysis, notifications to the French and EU authorities, defending clients against increasing enforcement actions (warning letters, seizures, product recall and withdrawal proceedings, inspections, administrative/criminal investigations, and penalties, as well as civil claims).
- Implementation of international anticorruption/sanction compliance policies under French law.
- Implementation of multijurisdictional compliance programs.
- Advice on EU and U.S. sanction issues.
- Corporate governance matters for both listed and unlisted companies (such as say on pay, gender parity within board of directors).

JONES DAY GLOBAL COMPLIANCE TEAM

Paris Team

Françoise S. Labrousse
Government Regulation, Environmental, Health & Safety
+33.1.56.59.39.39
flabrousse@jonesday.com

Eric Barbier de La Serre
Antitrust & Competition Law
+33.1.56.59.39.39
ebarbierdelaserre@jonesday.com

Jean-Michel Bobillo
Labor & Employment, Restructuring & Reorganization
+33.1.56.59.39.39
jmbobillo@jonesday.com

Thomas Bouvet
Intellectual Property, Patent Litigation Technology, Trade Secret
+33.1.56.59.39.39
tbouvet@jonesday.com

Alban Caillemer du Ferrage
Banking, Finance & Securities, Financial Institutions Litigation & Regulation, Financial Products Litigation
+33.1.56.59.39.39
acf@jonesday.com

Philippe Goutay
Financial Institutions Litigation & Regulation, Technology, Blockchain & Digital Currencies
+33.1.56.59.39.39
pgoutay@jonesday.com

Bénédicte Graulle
Investigations & White Collar Defense, Financial & Commercial Fraud, Internal Investigations, Cybercrime
+33.1.56.59.39.39
bgraulle@jonesday.com

Olivier Haas
Cybersecurity, Privacy & Data Protection, Intellectual Property, Technology
+33.1.56.59.39.39
ohaas@jonesday.com

Sophie Hagège
M&A, Joint Ventures & Strategic Alliances, Technology
+33.1.56.59.39.39
shagege@jonesday.com

Linda A. Hesse
Capital Markets, Mergers & Acquisitions
+33.1.56.59.39.39
lhesse@jonesday.com

Elie Kleiman
Global Disputes, International Commercial Arbitration
+33.1.56.59.39.39
ekleiman@jonesday.com

Emmanuelle Rivez-Domont
Labor & Employment, Business Restructuring & Reorganization, Internal Investigations, Corporate Compliance Programs & Employee Misconduct
+33.1.56.59.39.39
earivez@jonesday.com

Armelle Sandrin-Deforge
Government Regulation, Environmental, Health & Safety
+33.1.56.59.39.39
asandrindeforge@jonesday.com

U.S. Team

Karen P. Hewitt
Business & Tort Litigation, Investigations & White Collar Defense, Foreign Corrupt Cybersecurity, Privacy & Data Protection
+1.858.314.1119
kphewitt@jonesday.com

Henry Klehm III
Practice Leader Securities Litigation & SEC Enforcement
+1.212.326.3706
hklehm@jonesday.com

Christopher K. Pelham
Global Disputes, Investigations & White Collar Defense, Public Corruption Investigations
+1.213.243.2686
cpelham@jonesday.com

Europe Team (Outside France)

Renato Antonini
Government Regulation, International Trade & National Security
+32.2.645.14.19
rantonini@jonesday.com

Karin Holloch
Investigations & White Collar Defense
+49.211.5406.5500
kholloch@jonesday.com

Holger Neumann
Government Regulation
+49.69.9726.3939
hneumann@jonesday.com

Glyn Powell
Investigation & White Collar Defense, Global Disputes, Offshore Disputes
+44.20.7039.5212
gpowell@jonesday.com

Harriet Territt
Global Disputes, Financial Institutions Litigation & Regulation, Internal Investigations
+44.20.7039.5709
hterritt@jonesday.com

Middle East and Asia Team

Sean Thomas Boyce
Global Disputes, Investigations & White Collar Defense, Financial Institutions Regulation
+971.4.709.8416
sboyce@jonesday.com

Sheila L. Shadmand
Global Disputes, International Investigations
+971.4.709.8408
slshadmand@jonesday.com

Mathew J. Skinner
Global Disputes
+65.6233.5502
mskinner@jonesday.com

Peter J. Wang
Global Disputes
+86.21.2201.8040 / +86.10.5866.1111
pjwang@jonesday.com