COMPLIANCE WEEK
FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE



8 compliance challenges facing European companies in coronavirus crisis



By Neil Hodge | Thu, Mar 26, 2020 12:13 PM

With the exception of essential services, Europe is now at a standstill: In most European Union countries, companies have shut up shop, halted production, mothballed their operations, and sent their employees to work from home—if performing any kind of duties is still possible, that is.

The unprecedented impact the coronavirus pandemic is having on business has produced fresh concerns compliance officers need to address—and quickly.

While remote working poses practical problems, such as procuring enough laptops, ensuring connection quality is high enough, or even having enough food for employees still working on site now that restaurants and cafes are shut, operational changes are likely to result in serious legal and regulatory challenges.

Some regulators have recognized the burden companies may be under and have either relaxed certain rules or their expectations about how well organizations can comply with them. For example, in the United Kingdom, **the Information Commissioner's Office** has already confirmed it won't penalize companies for diverting resources away from usual data compliance to prioritize other immediate or higher-risk areas. The **U.K. government** has also relaxed some tax rules, as well as restrictions on businesses (such as supermarkets) working together where there is an absolute necessity.

Lawyers warn, however, these measures should be seen as a targeted, temporary fix, rather than a signal to start ignoring laws generally or to think enforcement will be put on the back-burner. "Companies are still liable for compliance failures," says Hermès Marangos, a partner at law firm Signature Litigation. "The virus emergency does not postpone or modify the law. There are no exemptions unless so provided by the legislation itself. Despite this, there are already individuals and entities trying to profiteer, behave unethically and contrary to laws and regulations in many instances."

Below experts spell out eight compliance challenges organizations are likely to face as Europe's lockdown continues:

1. Violations of competition law

Lawyers say that infringing competition law is an obvious "red flag" area companies and their compliance functions need to be aware of. While the two most likely areas of potential infringement remain abuse of dominant position and price-gouging (many EU competition regulators have already issued warnings and announced investigations), companies may also violate competition rules by collaborating too closely with competitors during the crisis—even if regulators, like the United Kingdom's Competition and Markets Authority (CMA), have relaxed the rules regarding cooperation to ensure better movement of essential supplies, such as foodstuffs and medicines.

"Companies still need to be aware that even if EU governments do want to relax the rules to enable closer coordination between competitors, it does not mean that competition law ceases to apply to the arrangements they put in place," says Matthew Hall, competition lawyer at law firm McGuireWoods. "Companies can still be found to have breached competition law, even if the government has seemingly sanctioned them by allowing closer cooperation."

2. Solvency risk

Cash is king—and ensuring smooth cashflow is going to be crucial to staying in business. European governments have committed to pumping billions of euros into propping up businesses and their economies, and the European Commission has relaxed state aid rules to allow them to do so.

Yet, despite such promises of cash injections, tax holidays, and employee salary payments, companies still need to be canny with the money they have. Keeping a tight hold on the purse strings, however, can present legal risks.

For example, hundreds of high street businesses in the United Kingdom have said they are not going to pay their upcoming quarterly rent bills, thereby breaching contract. Burger King Chief Executive Alasdair Murdoch said the fast food chain will not be paying rent due on its U.K. restaurants this week, while Richard Hodgson, chief executive of Yo! Sushi, told the *Financial Times* non-payment of rent was "not really a choice. It's just a basic piece of economics."

The government said shops will not forfeit leases if they do not pay, but they will have to pay arrears in the future. Landlords, however, have been less than enthused about the announcement.

The risk of insolvency should prompt compliance functions to look at their organizations' financial exposure and find ways of cutting costs, offsetting the risk, or renegotiating contract terms with suppliers and clients.

Stuart Evans, commercial litigation partner and specialist in business disputes and administration at law firm BLM, says organizations should "look critically" at the short- and mid-term predicament of their own business and commitments, whether mitigated by government measures or otherwise, using realistic projections, as well as look at what is happening to their customer base and supply chains.

"Look out for longer delays in invoices being paid, credit terms being re-negotiated, future orders dropping, news of redundancies or adverse changes," says Evans. "Is it time to look for new, more trustworthy suppliers that are testing their business as rigorously as you are? Do some customer accounts have to be put on hold? These are questions that need to be asked."

3. Due diligence risks

As companies are still legally liable for their own compliance failures and—in some circumstances—those within their supply chains, effective due diligence is still paramount, despite the obvious logistical problems.

Elizabeth Ross, associate managing director of business intelligence and investigations at risk consulting firm Kroll, says the need for due diligence "remains essential" as "times of market turmoil create opportunities to insert threats into supply chains via fraud or bribery and corruption weak spots, as well as intellectual property risk from unscrupulous partners. In the race to 'get the job done,' it's vital to continue to ask the right questions of potential partners and ensure standards remain high."

Some key areas where the "right questions" will still need to be asked are around "know your customer" (KYC) and anti-money laundering checks. But such monitoring will be made more difficult as firms implement working from home practices, which will no doubt impact a number of compliance processes designed around the ability to collaborate and work closely together as a team. These include alert remediation, information sharing, transaction monitoring, and reporting (including subject access requests, or SARs) plus paper-based onboarding processes, such as document reviews and KYC checks.

Michael Harris, director financial crime compliance at analytics provider LexisNexis Risk Solutions, says compliance teams will be under "considerable strain" due to additional pressure on their resources.

Harris believes meeting suspicious activity reporting obligations to both the regulator and to the financial intelligence unit is also likely to become more difficult with a remote workforce, "which is worrying given that fraudsters and scammers will already be working tirelessly to exploit the opportunities this crisis affords."

One area Harris thinks will likely see relaxation, however, is in customer due diligence (CDD) processes, as firms cannot reasonably expect customers to provide up-to-date documentation in current conditions. There will also likely be a let-up of strict customer exit procedures for the same reasons, he says.

4. Avoiding conflicts—and temptation

The coronavirus pandemic and subsequent lockdowns are creating compliance problems that would appear outlandish or even farcical in any other circumstance. Such risks, however, still need to be identified, mitigated, and controlled.

Paul Ford, CEO of Acin, a RegTech firm helping tier-one banks manage their operational risk and demonstrate compliance, says many financial organizations around the world are now being forced to look for creative ways to cope with their own challenges of managing decentralized teams as social distancing kicks in. This is particularly pronounced for bank trading rooms, he says, whose various responses carry huge compliance.

"Any company that maintains existing sales targets during this period is creating a significant risk of potentially corrupt behavior."

Angela Crawford, Partner, Crawford & Acharya

Yet, while remote trading raises the question of how phone lines will be monitored to detect illegitimate activity, strange times can produce stranger consequences: Ford is aware of a previously unheard-of situation where three traders are currently working remotely from the same London flat—all for different large banks.

Other traditional areas of conflict will also need to be re-examined for potential compliance failures: For example, the activities of sales and marketing teams must be checked—especially if their salaries are linked to sales bonuses.

"Any company that maintains existing sales targets during this period is creating a significant risk of potentially corrupt behavior," says Angela Crawford, a partner at law firm Crawford & Acharya. "For employees whose compensation may be severely impacted by COVID-19 disruptions, companies should consider adjusting sales targets and other KPIs to minimize any risk that employees may feel the need to resort to non-compliant behavior to meet pre-COVID-19 performance targets."

5. Staff shortages

As the pandemic spreads and employees fall ill and need to self-isolate, the availability of compliance professionals may be reduced, thereby causing further complications for businesses that need the function to assess new, emerging risks.

Richard Reichman, a partner at law firm BCL Solicitors, believes sectors providing "essential" services will come under particular pressure. This is because they may face increasing demand for their services, but as healthy employees become unavailable to work, they will need to ensure new employees are adequately trained, equipped, and

supervised to carry out the necessary work properly, with limited time to adapt to new compliance risks and difficulties.

John Binns, a partner at the same law firm, warns companies against thinking incidents of poor compliance due to poor resources and staffing will be looked at leniently by regulators. “The thresholds of ‘reasonable cause to suspect’ and ‘adequate/reasonable procedures’ haven’t changed: You might in some circumstances be able to fashion an argument that a drastically, quickly ‘cut down’ business should be able to relax its compliance function, but it would certainly face resistance from regulators and in the courts should it come to that.”

6. ‘Failure to prevent’ rules still apply

EU laws on “dirty money” and sanctions, as well as those in the United Kingdom that also find companies and/or directors liable for “failure to prevent”—such as the Proceeds of Crime Act, the Bribery Act, and the Criminal Finances Act—remain in full effect, “so a business is really taking serious risks if it closes its mind to these things when taking on new customers, suppliers, or partners, or dealing with money or property,” says Binns.

Nor should companies take comfort from any notion that regulators are under pressure and so will be less likely to enforce the rules, he says. “While there may be some truth in that for the short term, enforcement of the law is always going to be a priority for the state, even more so in a time of crisis,” says Binns. “It will be interesting to see whether in the longer term the direction of travel towards businesses enforcing the law against each other (suspicious activity reports, private prosecutions) continues, or whether the crisis will prompt the state to take a more direct role. I suspect we will see a combination of the two.”

7. Data risks

There is no doubt ensuring data protection and privacy is going to be of paramount importance and trying to achieve this will be a compliance nightmare for some organizations over the course of the next few months.

Some EU data protection authorities have taken a pragmatic approach to compliance and enforcement, saying they understand some organizations may need to divert resources away from data management to deal with other operational areas more directly impacted by the crisis. As with GDPR enforcement, however, companies should

not expect all EU data protection authorities to act in the same way or to share the same view.

Working remotely and from home presents several data protection challenges compliance professionals need to recognize and attempt to mitigate.

CCOs need answers to these five questions

Camilla Winlo, director at data protection and compliance consultancy DQM GRC, says compliance officers "will probably find themselves playing catch-up over the next months" as new technologies are deployed and processes are modified—most likely without much testing.

As a result, she says, there are five key questions compliance officers need answers to in order to prioritize their work:

1. What Data Protection Impact Assessments (DPIAs) need to be done? DPIAs are a great tool to help organizations collect their thoughts and information together. They can help you spot gaps in documentation that will cause issues later, as well as highlight the key risks in processes.

2. If new software and hardware has been rolled out, how much attention did the manufacturer give to "privacy by design?" Are these products and services secure and lawful by default, or do they need to be configured?

3. Has anything new got inside the security perimeter? This could include personal devices connected to domestic WiFi, as well as external hackers who have exploited relaxed perimeter controls to attack information systems directly.

4. What training gaps have opened up? Have processes changed, do individuals understand the new processes, and do they understand their role in controlling the risks in these new processes? Most importantly, are there any new opportunities for high-impact events to happen by accident, or any high-impact or probability risks that need to be controlled by individual action? What do you need to do to train people on this—what evidence should you collect and how should you monitor compliance?

5. How has governance been changed? Are the usual KPIs still relevant and is it still possible to report against them? Do the usual management reports still provide all the

information management needs?

—Neil Hodge

Firstly, employees may be using their own IT equipment that might be shared with other family members who are also confined to the same house. This raises the prospect of children—who are often more IT-savvy but less risk-aware than their parents—accessing Websites and material not be permitted within the confines of the office and circumventing/ignoring usual security protocols.

Secondly, the equipment may be old and may not have been regularly installed with the latest security updates/software patches that would normally alert users to potential malware or detect viruses. As a result, incidents of cyber-attacks and data breaches could escalate as the number of suspicious e-mails and phishing scams grow.

Thirdly, organizations may find themselves relying on apps, software, and collaboration tools such as Slack, Microsoft Teams, and Zoom, that they may have been reticent to adopt in the past due to compliance fears.

Fourthly, in highly regulated industries, such as financial services, it is especially important for organizations to collect, store, and archive all employee communications to ensure compliance and for use in any potential future investigation. Compliance functions will need to find a way of achieving this even while the workforce may be working remotely and on different platforms and devices.

8. Supply chain management risks

COVID-19 has brought unprecedented strain on global supply chains. No company, whatever its focus and business mix, will be unaffected. Disruptive factors may include a combination of geographic risk, lack of access to supplies of vital manufacturing inputs, logistical challenges, and personnel issues, among others.

Supply chain due diligence assesses a host of factors, including product safety, financial solvency, modern slavery/human trafficking concerns, and environmental compliance. All of these areas still require adequate assurance and strict compliance. If companies must quickly pivot to a new supplier without conducting appropriate due diligence, they potentially raise the prospect of legal risk to their companies, as well as health and safety risks to consumers.

Lila Acharya, a partner at law firm Crawford & Acharya, says "companies should anticipate that just as their own business operations are disrupted during this global crisis, so too are their suppliers' operations." For example, a company's suppliers may face issues in their own supply chain, struggle meeting financial requirements, or be forced to meet customer demand with a remote or reduced workforce. Such challenges and pressures may heighten the risk that suppliers may cut corners, fail to comply with what they see as less urgent regulatory requirements, or otherwise engage in misconduct as they work in triage mode.

If a company is facing supply chain or procurement disruption during this crisis, there is the possibility the business will face pressure to engage new suppliers without conducting the appropriate level of due diligence. To reduce potential risk, says Acharya, the legal department should review all new supplier contracts to ensure appropriate legal terms are incorporated, review supplier invoices and payments for any red flags or anomalies, and monitor conduct to ensure it complies with applicable regulatory requirements and contractual representations and warranties.

As the vast majority of corruption and bribery cases brought by regulators have involved misconduct by third parties, Acharya says robust third-party due diligence is going to be crucial during the pandemic crisis.

"Now is the time for companies to remind their employees of any supplier and third-party due diligence procedures that the company has in place," she says. "If there have been modifications made to the procedures as a result of the COVID-19 crisis, these changes need to be documented and clearly communicated."

"Employees should be saving required due diligence documentation in an appropriate electronic platform or database, so that compliance with the procedures can be audited," adds Acharya.

"The fact that most of the business is working remotely does not mean that they don't have to comply with the rules—it just means it might be slightly more challenging and time consuming," she says.

RATE THIS RESOURCE

Select your rating